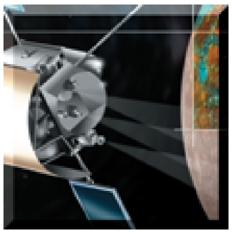


The System Approach to Successful Space Mission Development

Eric J. Hoffman and Glen H. Fountain

Conceptualizing and executing space missions calls for creative thinking coupled with careful and conservative implementation. The engineers and scientists who design such missions must master a "wide dynamic range" of techniques, from brainstorming to design reviews. Operating in space has never been easy, and the "better, faster, cheaper" mandate imposed by today's overconstrained budgets has created new complications. This article presents the Laboratory's philosophy for meeting these challenges. (Keywords: Space history, Space mission design, Spacecraft design, System engineering.)

INTRODUCTION

The APL Space Department has designed, built, and launched 58 spacecraft.[1] Another is in the final stages of integration and test, approaching launch, and three more are in early development. Three of our spacecraft—the Delta series—were developed jointly with another organization (McDonnell-Douglas), and one was integrated on a standard bus purchased from Orbital Sciences (the Far Ultraviolet Spectroscopic Explorer [FUSE]). APL spacecraft have ranged from the 53-kg environmental research satellite 5E-3 to the 2720-kg Midcourse Space Experiment (MSX), a 14-instrument "observatory class" spacecraft comparable in the scope of its instrumentation to the Hubble Space Telescope. APL helped pioneer quick-reaction spacecraft (a record possibly being the 75-days-to-launch Transit Research and Attitude Control [TRAAC]), invented many widely used spacecraft techniques, and developed entire space systems, such as the Navy Navigation System (Transit). Several important systems have been transferred to industry for production after being conceived and developed at APL, including Transit, the Global Positioning System Package (GPSPAC), and Geosat. More recently, APL has extended its "better, faster, cheaper" methodologies to low-cost interplanetary missions such as the Near Earth Asteroid Rendezvous (NEAR), Advanced Composition Explorer (ACE), Comet Nucleus Tour (CONTOUR), and MESSENGER.

In the course of all this activity, APL acquired a reputation for pragmatic and effective system engineering. Visitors often mention that *all* Space Department engineers seem to think like system engineers, whether or not they have that title. Perhaps less well known is APL's record of innovative, yet practical, advanced technology developments. Many of the standard techniques used on today's satellites were developed here.[2]

A small but prolific advanced technology development program continues that tradition today.

This article provides a top-level view of APL's mission development process, from mission objective to launch. Postlaunch operations and certain other aspects of mission development require the more detailed treatment given by the subsequent articles in this section. A strength of the APL Space Department has been our "end-to-end" approach to mission design and execution (Fig. 1). The close working relationship between space scientists and engineers fosters a symbiosis that is the hallmark of APL missions. Such closeness in a single organization is surprisingly unusual in the space industry; the fact that these two groups understand and empathize with each other—not just tolerate each other—is even more rare. The resulting ability to provide "one-stop shopping" for government space customers has contributed greatly to APL's record of success with better, faster, cheaper space missions.[3]

UNDERSTANDING THE PROBLEM

The article by Bostrom in this issue ("Defining the Problem and Designing the Mission") addressed the early concept and mission formulation phase. Every successful program must be able to state its *objective*, preferably in one concise sentence. (Possibly the best example of a concisely stated objective was President Kennedy's 25 May 1961 statement to a joint session of Congress: "I believe that this nation should commit itself to achieving the goal, before this decade is out, of landing a man on the moon, and returning him safely to Earth." It is important to remember that at the time Kennedy set out this bold objective, the United States had not yet orbited a single astronaut—John Glenn's first orbital flight was still 9 months away. Kennedy's single sentence not only stated the objective of what became the Apollo Program, it set forth the *schedule* as well!)

The objective isolates and pinpoints what is truly important; the value of a well-crafted objective cannot be overstated. It establishes the criteria by which mission success or failure will be judged, possibly many years down the road. It serves to periodically refocus the attentions of the team on the essential purpose of the mission, which might otherwise be forgotten in the forest of design details that accrue as time passes and as staff and subcontractors join and leave the program. Most importantly, it helps guard against "requirements creep," that deadly malady that has threatened more than one program.

The objective also isolates and emphasizes the essential kernel of *why* the mission is being done. Where does the objective come from? It can arise from a committee such as a science working group, user working group, or study team. But some of the most impressive breakthroughs have come from objectives set by a proverbial "wild-eyed sponsor," one champion obsessed with solving a particularly tough problem or performing a particular mission.

Once the top-level objective is established, a concept for meeting the objective is synthesized. That great system engineer Julius Ceasar provided the key to solving the really difficult, large problems: divide and conquer. The problem is broken down into smaller pieces, and subsidiary functional requirements are established, a process known as "requirements flowdown" (Fig. 2). This process of synthesis and analysis represents a very creative part of the mission design, with frequent iterations back and forth between alternative conceptual approaches, while keeping in mind the available *capabilities* and the numerous *constraints* (mass, schedule, cost, and a host of others). Deciding how to partition the system and where to establish the interfaces is almost an art form. Interface decisions made at this time can haunt (or bless) a program for its duration.

"Brainstorming" is one of the techniques used in this early stage of searching for conceptual solutions (see the section on The Design Process). Numerous books teach

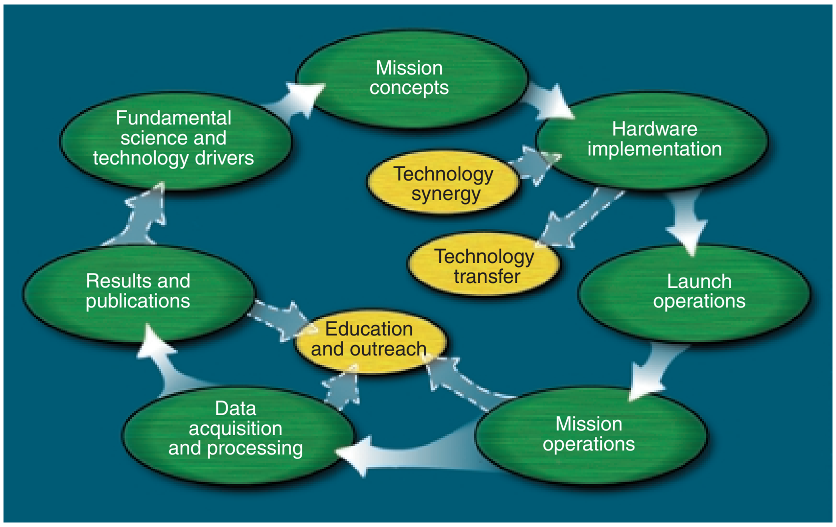


Figure 1. The APL Space Department provides complete end-to-end mission design and execution capability, fostered by the symbiosis between our scientists and engineers. A basic mission concept can be taken completely through development, launch, on-orbit operations, and analysis of the scientific data within a single organization, at substantial benefit to our government customers. At the same time, we are alert for opportunities to cross-fertilize technologies to other missions or transfer them to industry, and for education and outreach opportunities.

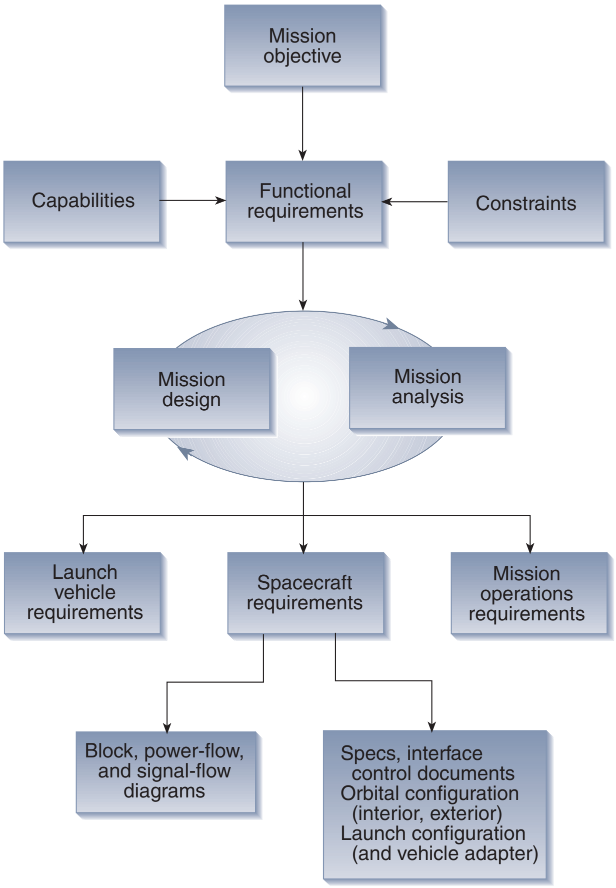


Figure 2. Starting with the all-important mission objective, top functional requirements are established, taking into consideration the available capabilities and the imposed constraints. A solution—the mission design—is synthesized by an iterative process of analysis and design. Subordinate requirements on the launch vehicle, spacecraft, and its subsystems, along with mission operations, are then "flowed down" from the top-level requirements.

brainstorming techniques and other useful conceptualization principles (see, for example, Refs. 4 and 5). A key to successful program management is the system stability that comes from an early freeze of the *functional* requirements. A worthy goal is to freeze them at the first system-level design review, typically the Conceptual Design Review.

In the course of this conceptual design process, the *system drivers* will become apparent. System drivers are major requirements whose satisfaction will establish one or more key attributes of the design. A spacecraft will often "look the way it looks" because of its system drivers. And system drivers are often highly leveraged: a small change in the requirement can lead to a big change in cost, schedule, or technical risk.

Once the top-level mission design concept has been synthesized, analyzed, and validated, the next level of functional requirements—for the launch vehicle, the spacecraft, the instruments, and mission operations—can be captured. Now, the familiar system engineering tools come into play: block diagrams, power and signal flow diagrams, specifications, interface control documents, and test plans.

The Delta 180 mission provides a good example of focusing on the true objective and meeting it through "out-of-the-box thinking." Soon after President Reagan challenged the military to develop a missile defense, the newly established Strategic Defense Initiative Organization (SDIO) wanted a quick and convincing demonstration of space intercept of a thrusting target. Various aerospace organizations proposed mission concepts, but they were all too long (3–5 years) and too expensive ($300–500M). One reason for the high costs was that all of these concepts envisioned separate launch vehicles for the target and the interceptor. APL system engineer Michael Griffin and program manager John Dassoulas considered the essence of the problem and came up with the novel idea of carrying both target and interceptor on a single, low-cost Delta launch. Furthermore, both spacecraft could be assembled from subsystems scrounged from various existing missile and launcher systems. SDIO accepted the concept, and the Delta 180 intercept was successfully carried out only 13 months from funded start, at a total program cost of $150M. Delta 180 received a presidential citation, two DoD distinguished public service medals, and awards from the American Institute of Aeronautics and Astronautics (AIAA), the American Defense Preparedness Association, and *Aviation Week & Space Technology* magazine. It was even popularized in *Reader's Digest*.[6] This demonstration of what could be done quickly, successfully, and at low cost for one government customer in 1985 started NASA thinking about its own "better, faster, cheaper" program.

ORGANIZING THE TEAM

One feature of APL's development process is the organization of teams. Each team has clear lines of responsibility for the execution of the mission, but in addition each team member has an understanding of other elements of the system. This widespread "system engineer thinking" results in a more robust system design, with the team retaining ownership of the entire process from concept to on-orbit operations. This culture—which is not as widespread in the aerospace community as one would expect—began with the Transit Program and can be seen today in the teams that produced ACE and NEAR and are working on missions such as TIMED (Thermosphere-Ionosphere-Mesosphere Energetics and Dynamics). This culture also reinforces the all-important ties between the scientists and engineers.

The article by Bostrom summarizes how the whole idea of Transit evolved from the work of George Weiffenbach, William Guier, and Frank McClure. Richard B. Kershner led the development of Transit, and it was his leadership and his choice of staff that set the tone for what followed. Kershner not only led, but actively participated in the development. He cajoled, challenged, and stimulated his colleagues as they tackled the various problems associated with the creation of one of the first practical and useful space systems. At the outset of the program he established a working group of the principal engineers and scientists, with himself as the "chief system engineer." In this role he saw to it that each member of the program leadership understood the problems in all of the constituent parts of the effort and created solutions in their area of expertise that took into account the effect on the system as a whole.

This divide-and-conquer process of parsing a system into component parts with well-defined interfaces and requirements, while keeping the requirements of the total system always in mind, resulted from Kershner's work in the early guided missile development activities at APL. Kershner was responsible for the development of the Navy's Terrier guided missile in the 1950s. To get reliable missiles built by the prime contractor, a process of well-defined subsystem requirements was implemented, with documented interfaces and a test program that ensured the integrity of each subsystem *prior to* integration. This methodology has been central to the Space Department's success throughout its history.

Resolving Conflict Among Many Requirements

NASA asked APL to use its expertise in small satellites developed for Transit to create a low-cost spacecraft bus capable of launch on the smallest operational launch vehicle, the Scout. By the time of the Small Astronomy Satellite (SAS) Program, the system engineering culture and the practice of delegating subsystem leadership and responsibility to lead engineers were firmly established. The development team used its system understanding to refine the mission requirements proposed by outside scientific teams into concepts that met the small size and low cost requirements. Four satellites—SAS-A through -C and Magsat—were launched in this series. In many ways, APL's work on the SAS Program anticipated the "reinvention," years later, of NASA's lightsat concepts of small, capable satellites and common, interchangeable buses.

Under the APL lead engineer concept, a single engineer has technical, cost, and schedule responsibility for a particular subsystem from concept to postlaunch. This includes conceiving the design approach; preparing a proposal; performing detailed design; defending the design at peer reviews; seeing the design through layout, detailing, and fabrication; performing qualification testing; assisting with integration onto the spacecraft; and providing postlaunch support. These tasks may transpire over a 2- to 3-year cycle and typically involve leading a small team of support engineers, technicians, and designers. The whole experience proves exciting and broadening to our engineers; it helps them see the big picture and start thinking like system engineers.

Forming the Engineering and Science Partnership

The Active Magnetospheric Particle Tracer Explorer (AMPTE, Fig. 3) exemplified the bridge between the science and engineering sides of the Space Department. The requirement to understand the effect of the space environment led to the establishment of a group interested in a large class of space physics problems. Early APL satellites flew instruments to answer problems directly related to Transit's needs. The instrumentation expertise developed in these investigations led to collaboration between APL investigators and colleagues at NASA and throughout the world. The scientists who developed the AMPTE mission concept were able to

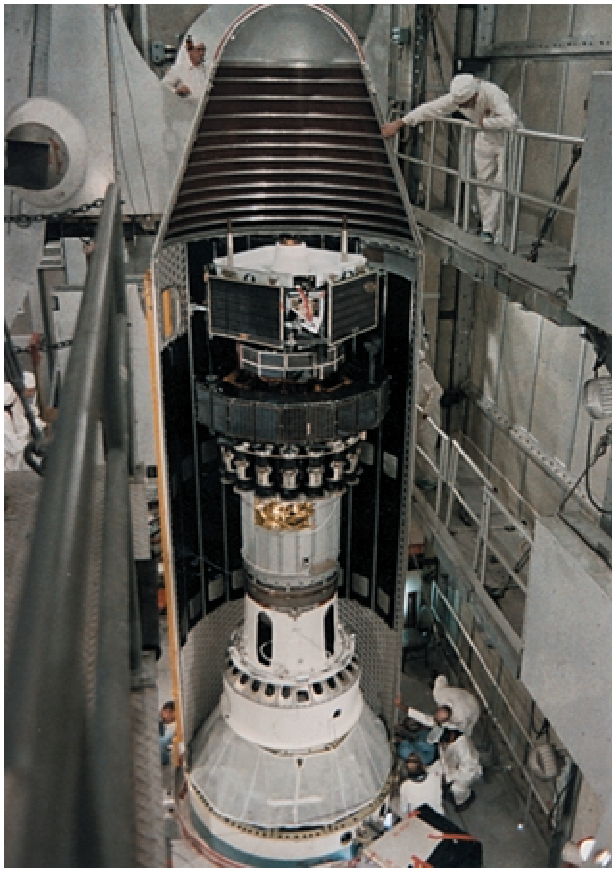


Figure 3. The AMPTE mission integrated science and technical teams in three countries to build the Charge Composition Explorer (APL), Ion Release Module (Max Planck Institute, Germany), and the United Kingdom Subsatellite (Rutherford-Appleton Laboratories and Mullard Space Science Center). The active nature of the science plan called for near–real-time measurement and control, and required the development of a real-time science data center. The interaction among the science team members, spacecraft developers, and mission operators was facilitated by APL's heritage of close cooperation between scientists and engineers.

draw upon the Department's engineering skills to develop and execute the mission. The Transit culture of using small, integrated engineer/scientist teams to define and lead the execution of a complex mission was easily adapted to the execution of this complex science mission, which involved the launching of three spacecraft at one time.

FABRICATION OF RELIABLE HARDWARE

The development of space systems requires that unique, one-of-a-kind units be fabricated and assembled with the quality of the best production line operations while retaining control of the cost. During the early years of the space program at APL, the fabrication processes were closely associated with the teams performing the engineering. Many space reliability investigations were conducted with the 5E series of spacecraft. The 1962 Starfish nuclear blast gave further impetus to understanding and defending against the radiation environment. To ensure that the systems developed by the Department were of the highest possible reliability, the detailed design, fabrication, and quality assurance functions were refined and staff with unique skills were recruited. These people eventually formed the core of today's Space Reliability and Quality Assurance Group as well as the Electronics and Mechanical Design and Fabrication Groups in the Technical Service Department. (These topics are treated more completely in Ref. 7 and in the article by Ebert and Hoffman, this issue.)

INTEGRATING "INTEGRATION" WITH OPERATIONS

The evolving complexity of space missions has driven the assembly and testing of the flight components and the development and testing of the operational ground segment into one activity. The primitive technologies and limited reliability available during the early days forced us to keep as much of the control and complexity of the mission as possible on the ground. We did in space only what *had* to be done in space, and then as simply as possible. A small number of measurements sufficed to verify proper spacecraft operation, and the rudimentary satellite designs had few operational states to test. For such missions, space and ground segments could be verified independently; there was little need to bring them together until shortly before launch.

Today's more complex missions demand more complex spacecraft. To keep this increased complexity from overwhelming the development process, the Department merged its integration and operations activities. The use of simulators for *both* ground testing and command upload verification (as on ACE, NEAR, MSX, and TIMED) is one positive outcome of the consolidation of these activities into a single functional group.

TIMED is taking integration one step further by providing seamless, independent operation of four instruments from four geographically separated organizations.[8] The development of this system entailed two requirements: (1) each instrument team had to have common ground systems that simulated the spacecraft interfaces, and (2) each team had to be able to interface their instrument's unique ground equipment to the simulator and ultimately (via the Internet) to the satellite operation facility. The mission operations plan allows the principal investigators at each institution to both support testing of their instrument and to operate it during flight from their home institution (Fig. 4).

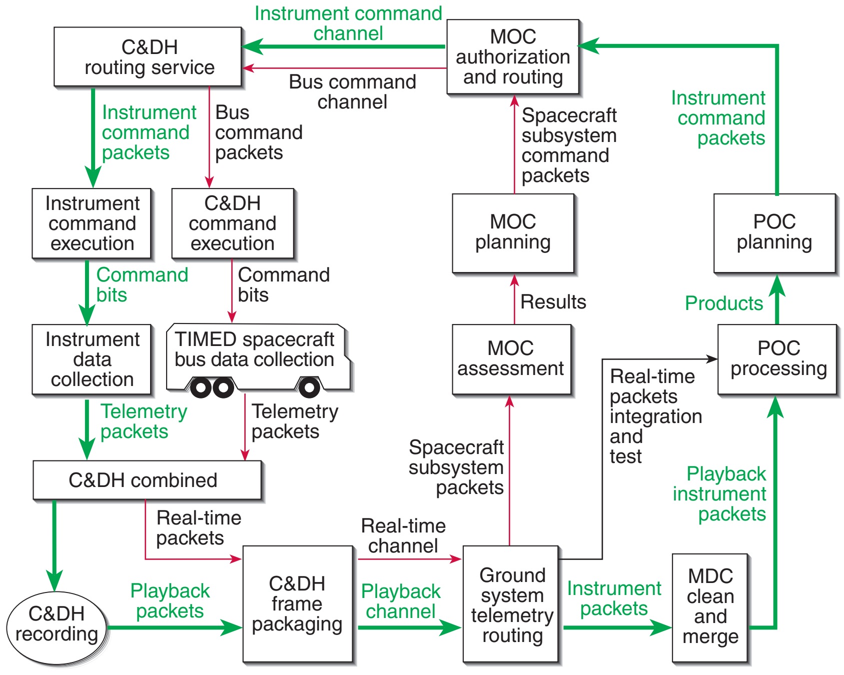


Figure 4. The TIMED operations concept relies on the ability of the spacecraft and its instruments to operate independently. Onboard status and data are downlinked to the APL Satellite Control Facility where instrument and spacecraft data are routed to the teams responsible for these different elements. Real-time or packetized data can be sent via local-area networks or the Internet. Each team will assess the data, plan future operations, and create appropriate commands at their home institutions. (C&DH = command and data handling, MDC = Mission Data Center, MOC = Mission Operations Center, POC = Payload Operations Center.)

THE DESIGN PROCESS

NASA and Air Force studies have shown that the single most important technical element of mission success is design. In one NASA study of more than 300 spacecraft and launch vehicle failures, design error was identified as the single biggest cause—the item simply was not designed properly in the first place.[9] The Laboratory had independently reached this same conclusion long before such studies were conducted and instituted a rigorous design integrity program that included a thorough design review process. Many of the details of this design integrity program are treated in the article by Ebert and Hoffman, this issue, and will not be repeated here. Suffice it to say that the list of considerations needed to achieve good design is a long one, and tight surveillance must be maintained on all of them in a balanced way.

The design process begins with a careful statement of the problem to be solved—the mission objective described earlier, or its subsystem equivalent. Focusing then on the *essence* of the mission objective, innovative solutions are often found by brainstorming, a special technique in which designers within a group play off each other's thoughts to create the largest *quantity* of possible solutions to the problem. Critiquing is strictly forbidden in a brainstorming session; the ideas will be sorted through and examined later. Once the "baseline" solution is selected, the "wild and crazy" brainstorming mode must give way to an extremely conservative, worst-case mindset for actually implementing the design. So between analyzing and synthesizing, brainstorming and critiquing, and worst-case designing, Space Department engineers are asked to operate over a wide dynamic range.

One of the most effective rules for achieving a reliable design is to "Keep it simple!" For example, a hallmark of APL spacecraft designs is the effort made to eliminate moving parts; thus NEAR differs from previous interplanetary spacecraft in that it uses a fixed (not gimballed) high-gain antenna, fixed (not rotatable) solar arrays, and no instrument scan tables.

A thorough, rigorous design review process is a key part of our design integrity program. The Department's design review requirements are one of several guidelines and standards set forth in the Space Department Engineering Notebook, which is accessible to all staff. Space Department design review practices receive favorable comments from outside organizations; in the ultimate compliment, NASA Goddard Space Flight Center (GSFC) adopted (with our permission) our guideline as their own internal standard.

With the key functional requirements established at the mission concept phase, the principal program documents cited earlier can be prepared. The Space Department approach uses the barest minimum of such documentation, but committing things to paper (or more likely today, its electronic equivalent) has two important advantages: paper "remembers," and the very act of writing things down organizes the engineer's thinking and exposes muddled logic. Often, especially in competed selections, a formal proposal will be required that may stipulate an exposition of the design similar to a conceptual design review level of detail. Preparation of such a proposal is a miniprogram in itself. At this stage, the system engineer is earning his or her keep by flowing down and apportioning requirements to the subsystems in a balanced way, keeping the mission objective foremost at all times. Of course, this flowdown takes place amid constant consultation with the subsystem lead engineers. Part of the system engineer's job is to "spread the pain evenly" in apportioning the requirements and resources; it's often said that a system engineer knows he has it right when all the rest of the team members are equally angry with him.

As flowdown proceeds, it is important to distinguish between true requirements and "desirements" (which are often best relegated to "goals"). For example, a classic system engineering error is to set the requirement to what someone said was "easy to achieve" rather than to the true minimal requirement as established by analysis. When, months later, it turns out that "easy to achieve" has become painfully difficult, no one may remember where the original requirement came from (the so-called "phantom requirement" problem). So requirements traceability, either kept in one's head or possibly managed by software, is an important part of the system engineer's job.

Mission conceptual design occurs within numerous constraints, one being the Space Department's policy on *margins*. For example, a mission design is considered viable only if it can show at least 20% margin on spacecraft dry mass at the conceptual phase. Similar margins apply to other important resources such as power, fuel, RF links, and processor memory and throughput. Some of these margin requirements taper down rationally as the mission approaches launch (required mass margin, in fact, going to zero at launch). Both NASA and the AIAA have subsequently adopted and formalized these tapered margin concepts.[10]

Good margin management is important not only to ensure the credibility of proposed new concepts but also to ensure solid engineering once the program is under way. An example of how insufficient mass margin seriously affected reliability is shown by APL's worst-ever in-orbit failure—the unsuccessful deployment of the Transit Improvement Program (TIP-2 and -3) solar arrays. After a long investigation, the failure scenario was determined to be as follows: the Scout launch vehicle heat shield was (intentionally) deployed at a lower altitude than normal. That, coupled with an unusually shallow angle of attack, caused aerodynamic heating, which in turn caused the "carpenter rule" antennas to melt to their nylon guides, thereby preventing the release of the arrays. But why was the heat shield deployed early in the first place? It was to deal with a lack of mass margin on the spacecraft!

An example with a better outcome shows how mass margin can rescue a mission. When NEAR's main engine burn aborted in December 1998 on entry to the target asteroid Eros, the recovery used much more fuel than anticipated. However, NEAR carried ample delta (fuel) margin by design. In addition, NEAR at launch had not zero mass margin but 6 kg. This extra mass margin allowed us to load extra fuel onto the spacecraft, and the extra fuel carried from this converted mass margin helped save the mission.

Eventually design must cease and fabrication (and coding) begin. To ensure correct implementation of the approved design, effective configuration management is necessary. The Space Department uses the APL-standard configuration management system operated by the Technical Services Department. This system is well documented, and the staff in both departments are familiar with its requirements. Like other APL systems, it offers multiple levels of control, four in this case. Therefore, every element of every program need not operate at the highest level of tightness of control for documentation and changes. The actual levels selected depend on the complexity and criticality of the program element. These levels are selected in advance and documented in the program's Performance Assurance Implementation Plan.

Understanding the Environment

Misunderstanding the environment is a favorite on everyone's list of why things fail in space. Much of APL's early Transit work was, in fact, devoted to understanding the space environment and its effects. Several of our early spacecraft were dedicated totally to measuring and understanding the space environment and laid the foundation for the Department's space science program.

Once past launch, the space environment can in some ways be more benign than many terrestrial environments (e.g., under the hood of a car). However, many subtleties and traps await the designer. One example is "cold welding," the phenomenon by which two parts made from the same metal, in intimate contact in the hard vacuum of space and without the adsorbed layer of oxygen they would have on Earth, stick to each other as if welded. The existence of cold welding is still controversial, but the APL-designed (RCA-manufactured) Nova-1 satellite (1985) seems to have encountered it. Nova's disturbance compensation system used a small cylindrical proof mass levitated around a wire. This sensor controlled microthrusters to null out drag and radiation pressure. After the system had been turned off for a month, the gold alloy proof mass appeared to have become "stuck" to the gold wire. It finally took a timed series of proof mass suspension current commands at the system's mechanical resonant frequency to break the cold weld loose.

The space radiation environment represents another unique challenge, affecting materials and, most especially, electronics. Total dose and single event radiation effects are the main reason why spaceborne processors lag typically 2 to 5 years behind their terrestrial counterparts. APL played a pioneering role in understanding the space radiation environment and learning how to design for it. The 1962 Starfish high-altitude nuclear blast demonstrated (unintentionally) how vulnerable satellites could be, impacting our Transit 4B and TRAAC as well as many other non-APL satellites. With the critical Navy Transit System to protect, APL soon became expert in designing not only for the natural radiation environment, but for the nuclear weapon "enhanced" environment as well (see Ebert and Hoffman, this issue, for a fuller discussion).

The Buy Versus Build Decision

One important early decision for each element of the spacecraft—even for the entire bus itself—is "build versus buy." By "build" we mean to produce within APL rather than purchase, and even this selection has two choices: to design from scratch or to "build to print" a prior APL design. The question is really therefore "design, rebuild, or buy?" A complex array of factors, both technical and managerial, must be considered. These include the obvious ones like cost, schedule, and performance and also such "soft" issues as staffing availability and the workloads in the Space and Technical Services Departments.

Designing and building in-house provides the very best control on quality and schedule. And—let's be honest about this—it provides more fun for our engineers. But in today's highly cost-constrained programs, we must make these decisions totally objectively. A "heritage" design (i.e., bringing over a design from a prior successful use on another program) can save time and money, but has its own set of pitfalls. To begin with, is the prior design sufficiently well-documented for a rebuild, and are parts still available? Second, what is *different* in this application (performance? interfaces? environment? what?)? In the early days, having a compatible *structure* for some new start-up was considered excellent heritage, as with the Geodetic Earth Orbiting Satellite (GEOS-A) to the DoD Gravity Experiment (DODGE). Today, it's software! But the space business is fraught with disastrous examples of misapplied heritage designs, the most expensive possibly being the incorrect reuse of a guidance software module on Ariane V's maiden flight—a $700M mistake!

Sometimes the sponsor will force the "design, rebuild, buy" decision for us: APL wanted very much to design and build the Magsat Attitude Transfer System, but NASA decreed that we subcontract it to industry. For GPSPAC, the first spaceborne GPS navigation system, APL wanted to design and build the GPS receiver/processor itself, but the sponsor directed that we subcontract it to industry.

The Laboratory also instituted a system to best use "heritage parts." In addition to our system for buying scarce flight parts on overhead and then selling them back at cost to programs (see Ebert and Hoffman, this issue), we long ago instituted an efficient way to transfer parts between programs. The Delta 180 Program was one of the first beneficiaries, buying many of its parts from AMPTE residuals. The reimbursement funds thus earned by AMPTE were then used to fund its Science Data Center. NEAR benefited similarly from MSX residuals, and the Jet Propulsion Laboratory used a variant of the system to sell Cassini residuals to Mars/Pathfinder. Despite providing a clear win–win situation for both programs, both government sponsors, and APL, this cost-reimbursement system is under constant scrutiny by auditors and is always in jeapordy.

Reliability Apportionment and Redundancy

Reliability apportionment and redundancy are key decisions that must be made early in the design of any system or subsystem. Few programs can afford the old method of simply specifying that "no single point failure shall cause loss of the system." Although easily stated, that requirement can be painfully difficult and expensive to meet, and then to validate through analysis, review, and test. In making redundancy trades, it is important to resist the temptation to simply add redundancy where it is easy or to make redundant those boxes that were made redundant on the last project. While hardly anyone today places much faith in the *absolute* numerical predictions of MIL-217–type reliability analysis, analysis of this type is, in fact, useful for conducting sensitivity analyses to show where additional reliability is needed and for comparing two different topologies, particularly redundant versus nonredundant.

Redundancy can involve more than simply adding a second box. Much of the effort in developing APL's Integrated Electronics Module (IEM), for example, went into ensuring failure-proof implementations of the signal backplane and power distribution to the individual cards. These architectural sophistications greatly increase the flightworthiness of the IEM and make it much more than just "a bunch of cards in a card cage." Sometimes the reliability requirement can be met by using functional redundancy instead of adding a duplicate box. For example, if a star camera should fail, its function might be accomplished, in a degraded way, by using a visible imager carried as part of the science payload.

Risk Management

"It's incredible how much bizarre stuff on Triad worked!" says John Dassoulas, Triad Program Manager. APL's Triad was the first satellite to fly a pure gravitational orbit, free of the drag and solar pressure perturbations experienced by all other satellites. It did this by flying a spherical proof mass in a shell, shielded from all nongravitational effects, and keeping the satellite centered around the proof mass by firing microthrusters. Triad was built in three parts separated by booms to control local gravitational attraction. And as if all this wasn't complicated enough, it was powered by a radioisotope thermal generator (RTG) power source. Yet, it worked perfectly. Likewise, the Delta 180 mission, designed and executed in 13 months and involving 2 space vehicles, 38 ground radars, 6 airborne observation posts, and 31 satellite links, performed the first thrusting space intercept flawlessly. How are such things possible?

It's been said that all of project management is risk management. *Risk* is the probability of some program element having an unfavorable result times the severity of the consequences (Fig. 5). A project can face technical, cost, schedule, or political risk. Technical risk—the subject here—can be evaluated in design reviews and in other formal, independent risk assessments. Probabilities are usually quantized to low, medium, and

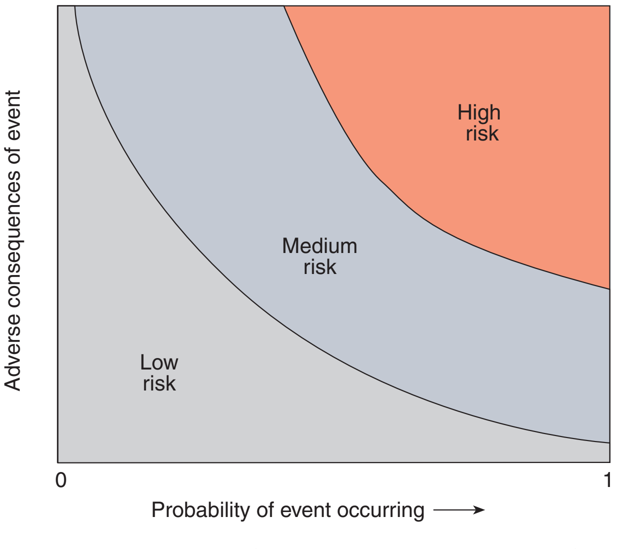


Figure 5. Expected risk of a particular item is the product of the severity of the consequences and the probability that it will occur. Once risk items are identified and rank-ordered, they can receive additional program surveillance or other risk mitigation actions.

high, and “traffic light” charts (green, yellow, red) can profile the risk areas on a complex program. High-risk areas, once identified, can be mitigated in a number of ways. Ideally, the risk area, or the design driver that created it, can be designed out of the system. Failing that, early risk reduction experiments, or building prototypes or engineering models, may provide an early assessment of the true risk. Extra margins can be carried for high-risk elements. Surveillance of the risk item will surely be increased. Finally, no program today is without its “descope plan”—a predetermined, prioritized list of features, or even entire subsystems, that can be deleted in a pinch. Descoping is obviously a last resort, but the later it is done the smaller the payoff. That is why *early* recognition of risks is so important.

Technical risk can result from reaching for unrealistic performance, beyond the state of the practice. It can arise from system complexity and the sheer number of interfaces. Changing requirements is a common source of risk, which is why an early requirements freeze is essential. Risk can arise at any stage where something can go wrong that sets the effort back: part orders wrong or late, components destroyed during fabrication, systems damaged in test, mission operations errors—the list is long. There is risk in the launch itself (about 3% of launches end in failure; in the early days it was 30%), and finally from lifetime and aging issues once in orbit. Modern risk management[11] attempts to organize and analyze semiquantitatively all of these risks and to mitigate them where economically feasible. In this way, risk management merely formalizes what successful program managers have been doing “in their head” for years. PERT (Program Evaluation and Review Technique) charts and critical path analysis are examples of risk management tools applied to scheduling.

In today’s programs, software development is invariably on the risk list. (The standard rule, for instance, is that software is *always* 90% complete.) The ability to reload software to modern spacecraft has, if anything, not helped because it now presents the irresistible temptation to deliver at least some of the software *after* launch. Seven years ago, the Space Department issued its *Software Quality Assurance Guidelines*[12] to bring uniform standards and discipline to software development, with different degrees of tightness of control depending on the risk. The success of this approach has been proven on such programs as MSX, whose 54 onboard microprocessors required the successful development of 280,000 lines of flight code.

EVOLUTION OF THE TECHNOLOGY BASE

The space program evolved a significant technology base to meet its own needs and produced countless technology spin-offs that benefit other sectors of the economy. The Space Department has made important contributions in this area, capitalizing on its tradition of identifying needs in new areas, or for different sponsors, that can benefit from solutions developed to solve past problems (Fig. 6). Working at the boundaries between differing problem sets promotes viewing new problems in different ways and is a proven approach to creativity.[5] APL’s history of transferring technology between DoD- and NASA-sponsored programs provides many examples (magnetic attitude control, heat pipe thermal control, autonomous onboard navigation, delayed commanding, etc.). There are, in addition, numerous examples of transferring these technologies into apparently unrelated areas, such as biomedicine and environmental assessment. This heritage of cross-fertilization and technology transfer provides an important element in the Department’s support of our customers.

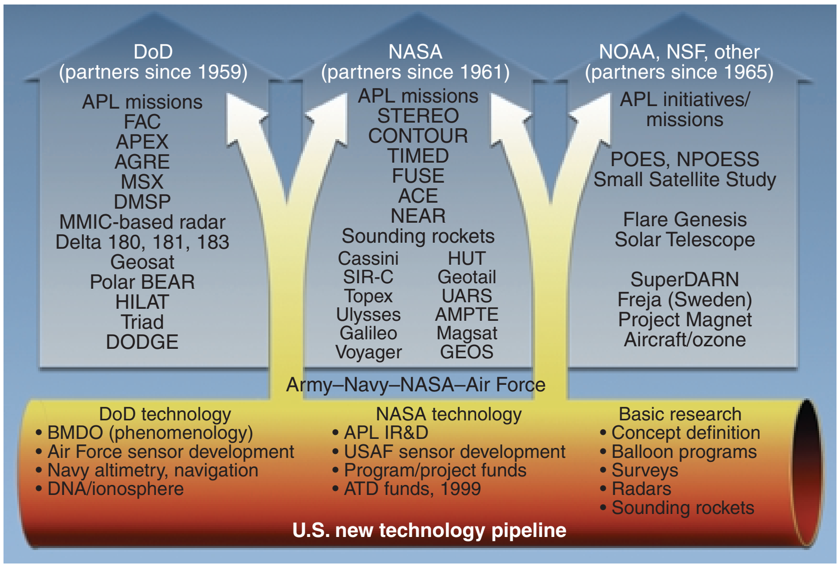


Figure 6. An element in the Space Department’s success across a broad range of missions is the ability to leverage and cross-fertilize technologies developed on different programs and for a variety of sponsors. (Acronyms not defined in the text are as follows: AGRE = Active Geophysical Rocket Experiment, APEX = Active Plasma Experiment, ATD = Advanced Technology Development, BMDO = Ballistic Missile Defense Organization, DNA = Defense Nuclear Agency, FAC = First Alert and Cueing, HUT = Hopkins Ultraviolet Telescope, MMIC = Monolithic Microwave Integrated Circuit, NPOESS = National Polar Orbiting Environmental Satellite System, NOAA = National Oceanic and Atmospheric Administration, NSF = National Science Foundation, POES = Polar-orbiting Operational Environment Satellite, SIR = Shuttle Imaging Radar, STEREO = Solar Terrestrial Relations Observatory, UARS = Upper Atmospheric Research Satellite.)

The development of ultra-stable oscillators (USOs) exemplifies the synergism across multiple sponsors of a critical technology and its value to the community. APL's USO development began with the need for a stable frequency source for the Transit Doppler navigation satellites and the realization that such a source could not be procured. A small team perfected the design, systematically balancing the circuit parameters, mechanical and thermal design, and the manufacturing processes.

Over the years the team improved the state of the art to meet ever-increasing performance demands from the technical community (Fig. 7). More than 400 APL flight oscillators have provided precise timing for navigation requirements and for probing the atmospheres of planets and their moons. The Laboratory is recognized as "the only credible source for [ultra-stable oscillators] when cutting-edge performance is needed" (personal communication, A. J. Kliore, Cassini Radio Science Team Leader, and C. L. Hamilton, Cassini Radio Science Instrument Manager, 23 Oct 1998). Until recently, the number of USOs required annually has been too small to make it a profitable commodity for industry. But the coming of constellations of satellites such as Iridium and Teledesic, with their need for precise timing, could soon change that.

Another area in which the Department has worked across sponsor boundaries to cross-fertilize the technology base is radar altimetry. Early work in this field was performed for NASA. But the early demise of NASA's Seasat left the Navy with a critical, unmet need in developing an improved gravity field model. The Department quickly responded to this need by developing the Geosat mission; the satellite performed flawlessly for 5 years. The latest in this series is APL's altimeter on the Topex satellite, which is currently providing data to study the El Niño/La Niña cycles in the Pacific Ocean. New requirements for altimetric measurements over global ice fields have led the Department staff to develop an entirely new class of instrument—the Delay Doppler Altimeter[13]—that combines two areas of radar science: classical altimetry and synthetic aperture radar (SAR). The instruments resulting from "working across the boundaries" have 10 times better along-track resolution and radiated power efficiency. The Delay Doppler Altimeter may enable missions as varied as ice measurements on Earth and on Jupiter's moon Europa and the future oceanographic needs of the Navy.

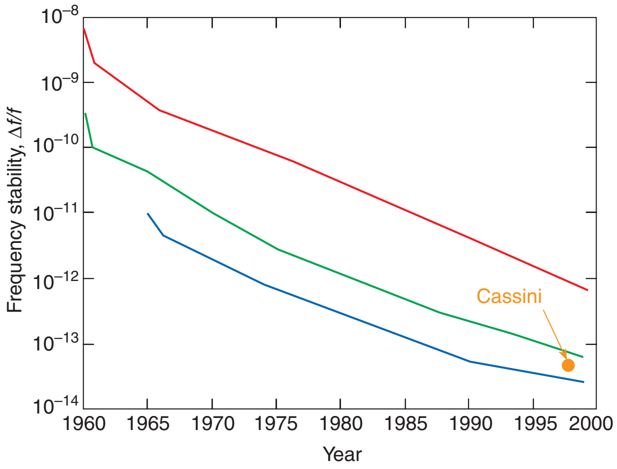


Figure 7. The stability of spaceborne quartz crystal oscillators has been steadily improved by the Department's technical staff in response to requirements for ever-increasing performance from a variety of customers. APL has delivered more than 400 flight oscillators for navigation, tracking, and radiometric science. (Red = aging rate, green = 1-s Allan variance, blue = 100-s Allan variance.)

INTEGRATION, TEST, AND LAUNCH OPERATIONS

Integration, test, and launch operations are the most exciting parts of any satellite program. At integration, the months of planning, design, fabrication, and subsystem qualification finally result in something that *looks* like a spacecraft. Testing is always interesting, often exciting (but it shouldn't be *too* exciting), and spiced with the occasional intellectual challenge of troubleshooting anomalies. And what can be more exciting than the final, fiery launch of your spacecraft into orbit?

Delivering a quality spacecraft requires careful and conservative design, rigorous independent review, meticulous assembly, and thorough testing. Each link in this chain must be strong. Protecting test time is always a challenge, especially as schedules get squeezed for "better, faster, cheaper" programs. But test we must, and it is a wise program manager who "fences off" and protects a substantial block of test time at the end of the program. As Orlando Figueroa, then Explorers Project Manager at NASA/GSFC, put it, "Test, test, and then test some more. Do it early."

One way to preserve schedule time for a thorough test program is to speed up the integration phase itself. APL's IEM, which carries nearly all the spacecraft bus electronics in a single card cage, and the R/IO (remote input–output) chip, provide examples of how this can be done. Besides eliminating a significant amount of time-consuming (and heavy) harnessing, when a flight-qualified IEM is delivered to the spacecraft, a substantial amount of integration and qualification has already taken place. Even spacecraft from our pre-IEM generation can make system decisions that speed up integration. With NEAR, for example, the entire propulsion system was purchased with its own substructure in order to save valuable integration time. The resulting mass penalty was less important than the schedule time saved.

How best to spend that test time is a subject of continual debate in the space community. Records of test failures, which are very difficult to obtain from other organizations, are constantly scrutinized to see which tests have the most payoff (Fig. 8). Testing has become even more complicated as we enter the era of large constellations of identical satellites like Iridium. Even smaller constellations (e.g., Transit), and now our four-spacecraft Auroral Multiscale Mission, have to address exactly what testing makes sense, especially for the 2nd through *n*th satellites.

The Space Department's test standards were first codified in the *Integrated Test Plan for Space Payload Equipment*,[14] a 1968 document that predates even the venerable MIL-STD-1540 Air Force test specification[15] (the current version is Ref. 16). A revised version of Ref. 14 (Ref. 17) is still the current test standard for our flight hardware and systems. This document establishes minimum mandatory tests that all Space Department flight hardware must meet, as well as a menu of recommended optional tests.

Particular attention is given to "protoflight" testing, recognizing that hardly any program today can afford the luxury of a full qualification model that does not fly. Under protoflight rules, the first unit built is the one that flies. Therefore, careful compromises in such factors as test levels and durations must be worked out to replace the previous qualification and flight tests.

The *order* of tests is important as well. For example, experience has shown that it always pays to perform the thermal testing *after* the vibration testing (which is also the order in which these environments are experienced during launch). A Space Department rule is "test what you fly, and fly what you test," i.e., the test article must be in flight configuration, or as close as possible, and other items cannot be added post-test (Fig. 9). For example, the last-minute NEAR fuel tank top-off cited earlier was made possible because NEAR had previously been vibration tested with 23 kg of extra mass in the fuel tanks. Our nuclear-powered Triad spacecraft had the first separable RTG heat source, a big safety innovation. But it meant that we couldn't strictly follow our policy to test what we fly (instead we used electric heaters to simulate the radioactive core).

Testing at the system level is preceded by a hierarchy of lower-level subsystem and instrument qualification tests, which help ensure that system-level tests are relatively trouble-free. We believe that this admittedly conservative approach lowers overall cost and schedule risk and contributes to APL's record of reliability in space.

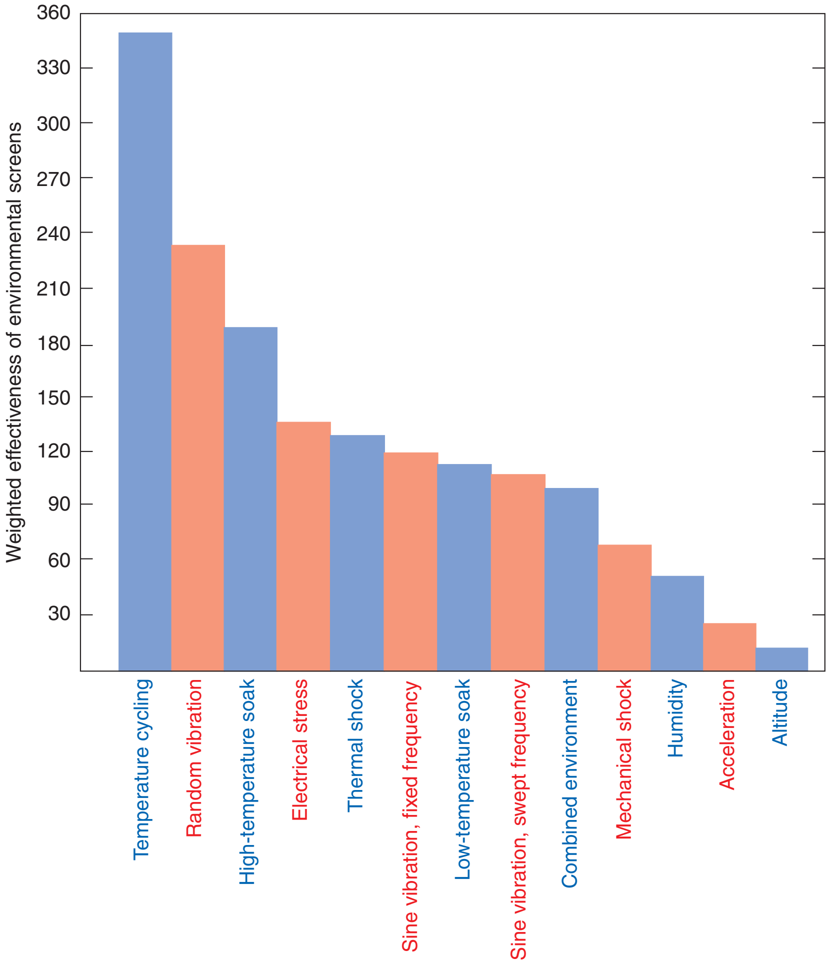


Figure 8. Testing time is precious, so it is important to know which tests have the highest payoff. The Space Department constantly monitors its own and external test data to see which tests provide the most benefit and determine the best order in which to conduct them. Space Department test standards are codified in Ref. 17.

LESSONS LEARNED

In any endeavor, but especially in space, it is important to learn from one's mistakes. Even better, of course, is to learn from *others'* mistakes! As Barry LePatner, attorney and witness before the House Subcommittee on Investigations and Oversight, put it in 1982, "Good judgment is usually the result of experience. And experience is frequently the result of bad judgment. But to learn from the experience of others requires those who have the experience to share the knowledge

Figure 9. The yo-yo despin mechanism being tested on APL's first satellite in 1959, under our philosophy of "test what you fly, fly what you test." James Smola (extreme right, now retired) is conducting the test.

with those who follow." Thus we have a tradition of figuring out and documenting "lessons learned" at the end of any major program or following any significant anomaly. The wise engineer and program manager will study these past lessons to prevent the ignominy of having to repeat them.

To some extent, the "better, faster, cheaper" era of starvation budgets and iron-fisted management has meant that we must absolutely get it right the first time. There is no room at all for cut-and-try. In a way, this robs engineers of the opportunity to stretch out, to take risks, and even, occasionally, to learn from failure. As Space Department founder Dr. Kershner is reputed to have said, "We haven't had a failure lately, so we're not learning anything." Balancing risky progress against stagnant perfection is a dilemma we all face every day in the space business.

BETTER, FASTER, CHEAPER

During the early years, back-up satellites were routinely developed as part of most space programs. NASA, in fact, sent all of its planetary spacecraft out in pairs until 1989. The level of risk in those days demanded that approach, and the budgets could support it. APL's first satellite, Transit-1A, was launched in the fall of 1959 but failed to reach orbit. The back-up Transit-1B was successfully launched in early 1960 and demonstrated the basic navigation concept. The Army-Navy-NASA-Air Force Program also built a prime and back-up satellite. Both were taken to Cape Canaveral for launch. During final checkout of the prime satellite, a fluctuation in the output power of a transmitter was observed. The back-up spacecraft was substituted *during the flight countdown on T – 0 day*; unfortunately, this launcher also failed to reach orbit. The original satellite was repaired and, when a second launch vehicle became available, was successfully put into orbit and operated for over 4 years.

Leftover subsystems or design elements were also regularly used in new ways to demonstrate new concepts. The TRAAC satellite was developed in only 75 days—possibly a record—using elements from the early Transits plus a few new elements like the first gravity-gradient extendible boom.

The close-knit teams at APL continue to transform basic designs into significantly different missions. The MSX spacecraft used a wide array of processors, sophisticated attitude techniques that enable rapid slewing and precise pointing and tracking, and many other important advances in instrumentation and communication. Many of the MSX design concepts and a few of the actual designs were transformed to form the core of the NEAR spacecraft. For instance, the MSX visible camera designs evolved into the NEAR Multispectral Imager. The X-band transmitter design was transformed into NEAR's X-band power amplifier. The control software for the NEAR Star Tracker was derived from the MSX tracker. NEAR also transformed APL's ultraviolet spectrographic imager design developed for Defense Meteorological Satellite Program (DMSP) satellites into an infrared spectrographic imager, saving precious time and money.

Being alert to the potential for transforming system elements from one program into the raw material for new, very different missions is a feature of the innovation process and a key "better, faster, cheaper" concept. The emerging space business environment is providing an even wider set of raw material to complement the Department's new concepts and internally generated technology. This view is formalized in the Department's overarching advanced technology goals, which include the concept of system scalability and the use and transformation of commercial off-the-shelf products.

LOOKING TO THE FUTURE

Space missions in the coming decades will require a different mix of skills and partnerships from those of the past 40 years. But the complexity of these new missions will still require the kind of system engineering viewpoint that has been at the heart of the APL culture. These challenging new missions will also continue to need mission-enabling new technologies.

The maturity of the space industry has resulted in a significant number of organizations that can provide systems and subsystems for many missions at lower cost than before. Reduced government space budgets are offset by this commercial activity, which is also providing new sources of technology investment. Both commercial and government programs contemplate many projects that require constellations of spacecraft where production line techniques are essential. Yet there remain a significant number of unique, one-of-a-kind, cutting-edge missions. Although their mission focuses differ, both government and industry will need new technology and elegant system solutions to meet their goals.

Two important shifts by the Department respond to this change in the space business environment and will significantly influence our mission development capability. These are an increased emphasis on advanced technology and the recent decision to perform research and development work for the commercial space industry. The type of cutting-edge science missions envisioned by Department scientists and their colleagues around the world as well as space-based solutions to national security needs will require new technologies. Cost constraints on all of these potential programs will also require elegant system solutions and the use of as much existing hardware and software as feasible. The rise of the commercial space industry provides opportunities to use a wider range of system elements, including commercially procured satellite buses, to enable these missions. Meanwhile, the opportunity to perform research and development for the commercial space industry may allow the Department to influence the types of system elements available for cost-constrained missions.

All of these scenarios will require the core competencies of the Department: the ability to take a system view of the mission, the science/engineering partnership, the ability to develop and exploit new and emerging technologies, and the hardheaded practical experience of the Department staff.

New tools are emerging that will help us develop these new missions. These tools include modeling and simulation advances as well as computer-aided design tools. Communications technologies allow the transmission of data sets to colleagues across the country so that engineers can merge design elements throughout the industry. These new ways of developing space missions have a wider reach and allow the deeper understanding necessary to execute the most complex missions, but at its heart it remains Dick Kershner's team of experts sitting around a table.

REFERENCES

[1] *Artificial Earth Satellites Designed and Fabricated by The Johns Hopkins University Applied Physics Laboratory*, S. J. DeAmicis (ed.), SDO-1600 (Revised), JHU/APL, Laurel, MD (May 1987).

[2] Hoffman, E. J., "Spacecraft Design Innovations in the APL Space Department," *Johns Hopkins APL Tech. Dig.* **13**(1), 167–181 (1992).

[3] Krimigis, S. M., Coughlin, T. B., and Cameron, G. E., "Johns Hopkins APL Paradigm in Smallsat Management," IAA-B2-0601, in *2nd IAA Symp. on Small Satellites for Earth Observation*, Berlin (12-15 Apr 1999).

[4] Logsdon, T., *Breaking Through: Creative Problem Solving Using Six Successful Strategies*, Addison-Wesley, New York (1993).

[5] Koestler, A., *The Act of Creation*, Hutchinson, London (1964).

[6] Bennett, R. K., "Triumph at Pad 17," *Reader's Digest* (Jul 1987).

[7] Wagner, G. D., "History of Electronic Packaging at APL: From the VT Fuze to the NEAR Spacecraft," *Johns Hopkins APL Tech. Dig.* **20**(1), 7–21 (1999).

[8] Cameron, G. E., and Grunberger, P. J., "System Engineering of Cost Efficient Operations," in *Proc. Fourth Int. Sym. on Space Mission Operations and Ground Data Systems (SpaceOps* 96), SO96.8.003 (Sep 1996).

[9] Williams, W. C., "Lessons from NASA," *IEEE Spectrum*, 79–84 (Oct 1981).

[10] *AIAA Guide for Estimating and Budgeting Weight and Power Contingencies for Spacecraft Systems*, ANSI-approved AIAA Standard, ISBN 0-930403-86-X (1992).

[11] Brown, I., Longanecker, G. W., and Madden, J. J., *Risk Assessment for Space Flight*, Applied Technology Institute, Clarksville, MD (Jan 1998).

[12] Lee, S. C., Hoffman, E. J., and Utterback, H., *Space Department Software Quality Assurance Guidelines*, SDO-9989, JHU/APL, Laurel, MD (22 Oct 1992).

[13] Raney, R. K., "A Down-Looking Satellite SAR with On-Board Real-Rate Processing: The Delay/Doppler Radar Altimeter," in *Proc. EUSAR '96*, pp. 189–192 (1996).

[14] Eckard, L. D., Jr., Wingate, C. A., and Frain, W. E., *Integrated Test Plan for Space Payload Equipment*, SDO-2387, JHU/APL, Laurel, MD (1 May 1968).

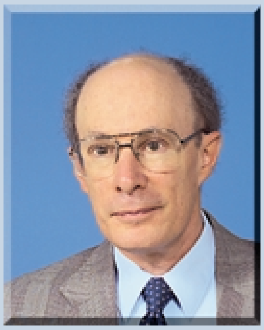
[15] *Test Requirements for Launch, Upper-Stage, and Space Vehicles*, MIL-STD-1540 (15 Apr 1974).

[16] *Product Verification Requirements for Launch, Upper Stage, and Space Vehicles*, MIL-STD-1540D (15 Jan 1999).

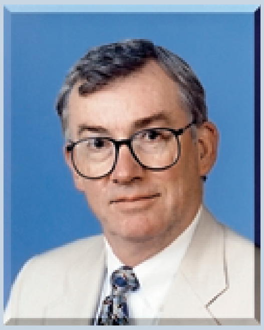
[17] Nagrant, J., *Integrated Test Specification for Space Payload Equipment*, SDO-2387-1, JHU/APL, Laurel, MD (Feb 1982).

ACKNOWLEDGMENTS: The authors are grateful for the information and "war stories" provided by members of the Space Department staff. We are especially indebted to John Dassoulas for his amazingly nonvolatile memory and willingness to share his recollections.

THE AUTHORS



ERIC J. HOFFMAN received degrees in electrical engineering from M.I.T. and from Rice University, and joined APL in 1964. He has performed system engineering for many of APL's space communication and navigation systems, as well as for entire spacecraft. He has supervised communications and navigation design activities and led satellite conceptual designs. As Space Department Chief Engineer, he provides technical guidance for Department programs, promotes system engineering, and sets standards for design integrity, design review, configuration management, and test. Mr. Hoffman has taught space systems design courses at the Naval Academy, The Johns Hopkins University, National Taiwan University, NASA, and NSA. He has authored 60 papers on these topics and is a co-author of *Fundamentals of Space Systems*. Mr. Hoffman is a Fellow of the British Interplanetary Society and an Associate Fellow of the AIAA. His e-mail address is eric.hoffman@jhuapl.edu.



GLEN H. FOUNTAIN received his B.S. and M.S. degrees in electrical engineering from Kansas State University in 1965 and 1966, respectively, and joined APL's Attitude Control Group in 1966. During his career at APL he has held a number of appointments and supported a range of programs including the Small Astronomy Satellite Program, the Transit Improvement Program, and Magsat. As Supervisor of the Space Science Instrument Group he led the ultraviolet and visible instrument developments for the Delta series of missions. Mr. Fountain was the Program Manager for the Hopkins Ultraviolet Telescope in the 1980s and the Special Sensor Ultraviolet Spectrographic Imager in the early 1990s. He is currently the Supervisor of the Space Department's Engineering and Technology Branch. His e-mail address is glen.fountain@jhuapl.edu.