The Application of APL Systems Engineering Discriminators to NASA Missions in the Space Department

David Y. Kusnierkiewicz and Glen H. Fountain

The APL systems engineering practices have been applied to NASA missions of exploration beyond the Earth–Moon system beginning with the first Discovery-class mission, Near Earth Asteroid Rendezvous (NEAR), which was launched in 1996. Since then, these practices have enabled missions to explore the ends of the solar system, from Mercury to Pluto, at lower cost than was previously thought possible. This article discusses the challenges presented by the MErcury Surface, Space ENvironment, GEochemistry, and Ranging (MESSENGER) mission to Mercury and the New Horizons mission to Pluto and illustrates how the APL systems engineering discriminators were applied to address these challenges. Both missions are characterized by significant technical challenges and programmatic constraints; bringing these missions to fruition requires close coupling between the technical teams, program managers, the sponsor, external partners, and other organizations. Lessons learned from previous programs were applied to both of these missions, and the experience gained from them is being incorporated into programs currently under development, furthering our ability to continue to make critical contributions to these critical challenges.

INTRODUCTION

Space flight missions have always presented unique challenges. By the early 1990s, the planetary science community was at an impasse. The high cost of missions had reduced their number, other than missions to Mars, to about one per decade. The Near Earth Asteroid Rendezvous (NEAR) mission demonstrated to the planetary science community (and to NASA) that credible science could be performed at moderately low cost with less complex spacecraft than "flagship"-class missions such as Voyager, Galileo, and Cassini. This result was achieved by working with members of the community to generate a disciplined set of requirements that could be implemented at lower cost. The NEAR mission's success enabled NASA to create Discovery, a new program that funded a series of low-cost planetary missions [including the MErcury Surface, Space ENvironment, GEochemistry, and Ranging (MESSENGER) mission to Mercury].

The initial projects under the Discovery program were characterized by the "faster, better, cheaper" execution mode. These projects raised the bar for scientific return per dollar expended in planetary exploration. While the faster, better, cheaper way of doing business has been moderated, so also have the "low-hanging fruit" been harvested; i.e., the "easy" planetary missions have been done. The challenges associated with space exploration under NASA's Discovery and New Frontiers programs remain formidable. These missions seek to maximize science return in the face of tightly constrained programmatic (cost, schedule) and technical (mass, power, etc.) resources. Meeting these challenges requires multiple systems engineering trades within multivariable trade spaces to optimize the system design.

The systems engineering construct for space science missions can be thought of as an essential element of the general APL systems engineering "loop" (see the Guest Editors' Introduction in this issue). As Fig. 1 shows, engineering teams led by a mission systems engineer work with members of the science community to "flesh out" concepts and, after initial functional decomposition, assess the feasibility of the concept to fit within the programmatic (schedule, cost, technology readiness, risk tolerance, etc.) and environmental constraints. System trade-offs are made in this process. For space missions, trades are typically made among mass, power, mission safety, technology risk, operations cost, launch capability, etc. For these missions, the interaction between programmatic and technical elements is very strong. Once an initial assessment is made that a design meets the constraints, the concept is refined and proposed (for science missions, the proposals are typically to NASA). If approved for advancement into the formulation phase, the requirements are resolved to a higher level of detail, and the system parameters may be revised before final implementation. Deployment (the flight or mission operations phase) results in the requisite science data collection and publication in the literature (the final product). Questions raised by the data complete the systems engineering loop.

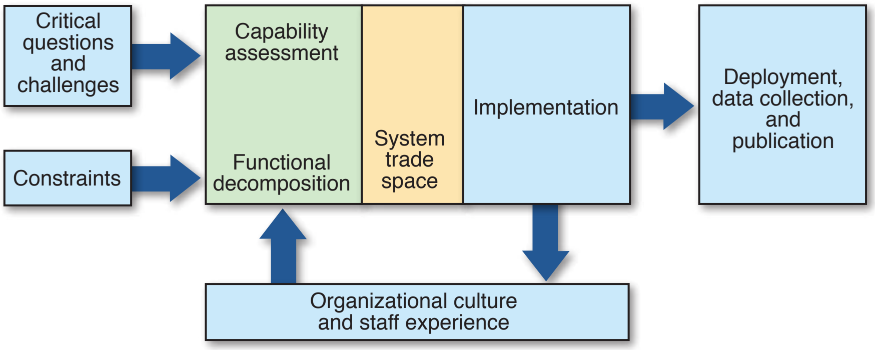
Critical questions and challenges
Constraints
Capability assessment
Functional decomposition
System trade space
Implementation
Deployment, data collection, and publication
Organizational culture and staff experience

Figure 1. Systems engineering activities are critical elements in both assessing a concept by functionally decomposing concept elements and studying trade-offs to determine whether a potential parameter set meets the mission constraints. The resulting concept allows APL to implement a system that provides the data to answer critical scientific questions.

These systems engineering trade studies draw heavily on the experience and expertise of our engineering staff and are inevitably dependent on the organizational culture. Interactions between the scientists and the engineering staff have resulted in innovative concepts that have enabled missions otherwise considered infeasible because of cost or technical constraints. Major innovations like those that enabled the NEAR mission have been made by asking critical questions about the perceived mission requirements and by making trades not previously thought within the trade space.

The "system perspective" we try to instill in our technical staff facilitates the execution of these trades, because the lead engineers supporting these studies are not confined to narrow, parochial thinking. Organizationally, the project and department management seek to continue to inspire the development and creativity of our staff. Balance is also sought with the risk tolerance of our NASA sponsor. The close coupling of science, systems engineering, and program management, along with our hands-on experience and understanding of the operational environment, enables our unique contributions. In addition, the organization must learn from the work it does to improve the processes it uses, thus becoming more effective in future endeavors that may present greater challenges than those faced in the past. The knowledge gained from past NASA missions, such as NEAR and the Comet Nucleus Tour (CONTOUR), is fed forward into MESSENGER and New Horizons and to future missions.

This article illustrates how APL systems engineering discriminators have been applied to the NASA MESSENGER and New Horizons missions to Mercury and Pluto, respectively.

CRITICAL CONTRIBUTIONS TO CRITICAL CHALLENGES

Both MESSENGER and New Horizons demonstrate the critical contributions made by APL to these critical challenges in solar system planetary exploration. Both are missions of true discovery, meant to expand the understanding of our world. The last NASA mission to

Mercury occurred more than 30 years ago, and a Mercury orbiter has never been achieved. APL was able to leverage our strengths in science and systems engineering, our previous experience, and our application of prototyping, test, and evaluation to support technology and engineering development that enabled the MESSENGER mission. Launch mass constraints, as well as the extreme thermal environment around Mercury, necessitated engineering developments in the lightweight spacecraft structure, the thermal protection sunshade, solar arrays, and communications antennas. Because the survival of the spacecraft depends on maintaining the proper orientation with respect to the Sun, demands were also placed on the onboard fault protection system to quickly execute proper safing procedures in the event of anomalous spacecraft attitude.

The erstwhile planet Pluto is the only planet in our solar system that has not yet been visited by a spacecraft. While the propulsive energy required to perform a Pluto orbiter mission is excessive, the New Horizons flyby mission and spacecraft are designed to maximize the science return from this once-in-a-lifetime opportunity. The launch opportunities available to New Horizons in 2006 and 2007 (New Horizons was launched during the first available window in January 2006) were literally the last opportunities in our lifetimes to visit Pluto using existing technology. While New Horizons presented many different challenges than MESSENGER, the New Horizons approach minimized technology development to minimize the associated risk of schedule delay. And, because the data required for mission success are obtained during a one-time flyby, during which ground intervention is not possible owing to the long round-trip light time (9 h), the onboard fault protection system was designed to continue science data collection in the event of spacecraft anomalies.

OVERVIEW OF SPACE MISSION DEVELOPMENT

NASA space missions are generally separated into two main divisions: Formulation and Implementation. Formulation breaks down into three phases:

- Proposal Development/Pre-Phase A: Concept studies
- Phase A: Concept and technology development
- Phase B: Preliminary design and technology completion

Implementation consists of four additional phases:

- Phase C: Final design and fabrication
- Phase D: System assembly, integration and testing, and launch
- Phase E: Operations and sustainment
- Phase F: Closeout

The MESSENGER and New Horizons projects began with proposal submissions in response to a NASA-issued Announcements of Opportunity (AOs). Both projects are run in the “Principal Investigator (PI) mode,” in which the project is awarded to a single individual, the PI, who is responsible for the entire mission. The PI partners with an institution such as a NASA center or APL to execute the mission. Dr. Sean Solomon of the Carnegie Institution of Washington is the PI for MESSENGER. Dr. Alan Stern of the Southwest Research Institute is the PI for New Horizons.

NASA funds worthy proposals to complete Phase A (concept development). Several competing concepts may be funded for concept development. To minimize overall project risk, a technology development plan must also be formulated in Phase A to show a credible path to an acceptable level of technology maturity by the end of Phase B. In the case of MESSENGER, and to a lesser extent New Horizons, significant technology development occurred during the proposal development and in Phase A.

MESSENGER SYSTEMS ENGINEERING CHALLENGES

MESSENGER will be the first spacecraft to orbit the planet Mercury, and it is the first NASA mission to Mercury since Mariner 10, launched in 1973. Mariner 10 did not go into orbit around Mercury, but it imaged ~45% of the planet’s surface during three flybys beginning in March 1974. An orbital mission to Mercury was not feasible using existing chemical propulsion systems before the discovery of trajectories that used gravity assists from Venus and Mercury to slow a spacecraft down enough that it can be injected into Mercury orbit.[1]

While these gravity assist trajectories brought a Mercury orbiter mission into the realm of the possible, they did not make it easy by any means. APL first proposed a Mercury orbiter under the NASA Discovery Program AO in 1996 (the third Discovery AO), but it was not selected. Encouraged to submit again, MESSENGER won the next Discovery opportunity in 1998, making it the fourth Discovery mission. Missions under this Discovery AO are focused science missions that must be accomplished for no more than $299 million (FY1999 dollars), including launch services. The Boeing Delta-II was the most capable launch vehicle available for Discovery.

A Mercury orbiter mission presents the following driving challenges:

- Constraints on launch mass
- Extreme thermal environment
- Solar array performance at close solar distances
- RF communications
- Spacecraft fault protection

After the first MESSENGER proposal in 1996 was not selected, APL undertook a number of risk-reduction activities. NASA is extremely cautious when awarding a mission: uncertainties in meeting technical, cost, and schedule performance raise red flags to proposal evaluators. Uncertainties require unallocated margins (mass, power, budget, schedule, etc.) commensurate with the risk. Two of the largest technical challenges on MESSENGER were the constrained launch mass (exacerbated by the large spacecraft fuel load) and the extreme thermal environment. To reduce uncertainty in the mass estimate and demonstrate acceptable mass margins, APL matured the design of the spacecraft composite structure to a point not usually achieved until the end of Phase B (preliminary design). Preliminary evaluations of thermal sunshade materials were also performed to demonstrate a solution to the challenging thermal environment, lending further confidence in the success of the mission concept.

Mass

The Delta-II 7925H launch vehicle could accommodate a maximum spacecraft mass of 1107 kg for the MESSENGER trajectory to Mercury. The trajectory design required the spacecraft to provide an onboard propulsive capability of 2700 m/s (post-launch change in velocity, ΔV). This ΔV requirement translated into an onboard fuel requirement of about 600 kg, or about 54% of the spacecraft launch mass. It is always desirable to minimize the mass and power requirements of the spacecraft bus in order to maximize the availability of these resources for the scientific instruments. (The mass of the MESSENGER science instruments was 40 kg.) The MESSENGER engineering team undertook new designs in several areas to accomplish this.

The spacecraft structure was one area of mass savings. Traditionally, spacecraft structures have been made mostly of aluminum. The rule of thumb is that aluminum structures consume 12–15% of the spacecraft launch mass, or as much as 160 kg for a 1066-kg maximum launch mass. The MESSENGER mechanical design team developed a structure design using a graphite/cyanate ester (GrCE) composite material instead of aluminum. In addition to the mechanical properties of the structure, thermal and electrical grounding (for electromagnetic compatibility) requirements were also taken into account. The structure design was also closely coupled to the design of the propulsion system to make the most efficient use of available mass. The propulsion system was integrated into the structural design, as opposed to a modular design, which is less mass efficient. Thus structural stiffness and strength, thermal properties, electromagnetic compatibility, and propulsion system performance were all driving inputs into the structure design. The team did far more detailed design and analysis than is usually performed early in the proposal phase to prove the credibility of their 75-kg (a 7% mass fraction) mass-saving design.

Mass savings were also realized through a redesign of the spacecraft electronics. Heritage units from previous missions were too heavy for the MESSENGER mission. The mass of the MESSENGER main avionics unit was reduced by 40% from previous APL heritage versions.

Thermal Environment

The most obvious spacecraft design driver for a mission to Mercury is the thermal environment. The distance between Mercury and the Sun ranges from 0.31 to 0.46 astronomical units (AU) (1 AU is the average distance between Earth and the Sun, ~150 million km). During the cruise to Mercury orbit insertion, the spacecraft made its closest approach to the Sun, at 0.3 AU. At this distance, the intensity of the Sun is about 11 times brighter than in Earth orbit. The spacecraft design was required to accommodate the thermal and solar illumination environment between the extremes of 1 AU (launch) and 0.3 AU.

During orbital operations, the MESSENGER spacecraft will be in a high-inclination (inclined at 80° to Mercury's equator) elliptical orbit ~200 × 15,000 km with a 12-h period. At the 200-km altitude, thermal radiation from the surface of the planet provides significant heat input into the spacecraft. To keep the spacecraft temperatures within normal operating limits, MESSENGER's orbit is designed to limit the time spent at such low altitudes to less than 25 min out of each 12-h orbit.

The intense solar environment required specialized thermal designs for the solar arrays, telecommunications antennas, digital sun sensors, the spacecraft bus, and the onboard fault protection. These nonstandard designs required significant prototyping, testing, and evaluation to develop the required techniques and technologies.

The MESSENGER spacecraft bus is protected from direct solar illumination and resultant heating by a ceramic-cloth sunshade (see Fig. 2). Although the Sun-facing side of this protective shield will rise to temperatures above 300°C, the environment for the electronics behind the sunshade is kept near room temperature, a benign 20°C. The sunshade uses materials that are inherently tolerant of high temperatures, but the actual configuration of the multilayer structure required numerous solar simulation tests at a special facility maintained by the NASA Glenn Research Center (GRC), which is capable of simulating an 11-Sun environment. The GRC facility was able to accommodate simultaneous testing of the MESSENGER sunshade, solar array, antenna assembly, and digital sun sensor.[2]

The thermal environment also required innovation in the potential options for the RF communication system. The spacecraft must always be oriented with the heat shield toward the Sun, and thus the antenna implementation must be more agile than usual. A pair of electronically steered phased-array antennas (also

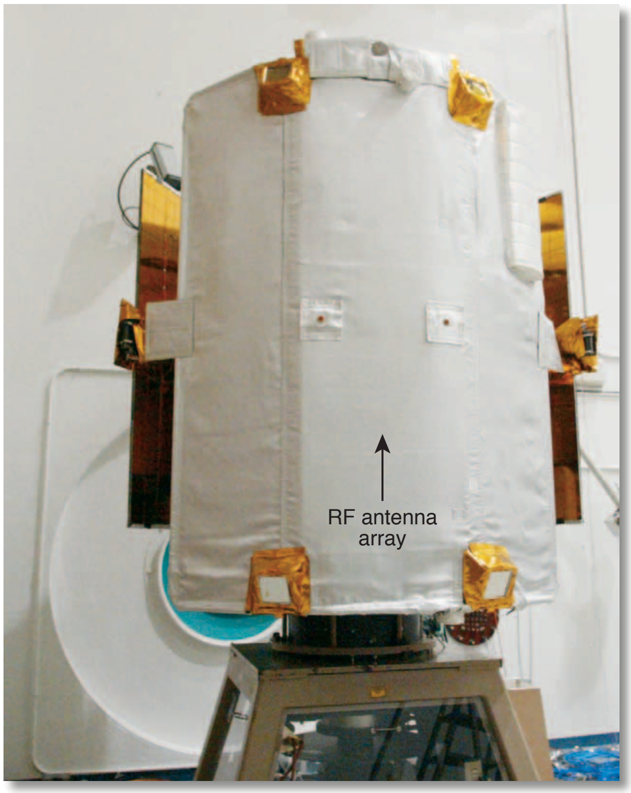

Figure 2. The MESSENGER sunshade, which protects spacecraft components from the harsh thermal environment at Mercury.

shown in Fig. 2) is used on the MESSENGER spacecraft to meet this constraint—the first application of such an antenna for deep-space communications. The antenna arrays are mounted on opposite sides of the spacecraft body, and they require no deployment mechanisms. Because they are steered electronically, no gimbal mechanisms or other moving parts are required. A high-temperature radome over the array keeps the antenna temperatures well below 300°C. The radome creates an infrared cavity for the array, maintaining a uniform, benign temperature environment. Without the radome, the antenna elements would be at risk of warping and distortion, degrading their performance.

Solar Arrays

The MESSENGER solar arrays must operate over the entire range of spacecraft-to-Sun distance of 1–0.3 AU. In addition, they must withstand the severe near-Sun operating temperatures. Producing a flight-worthy design again required considerable analysis of the range of operating environments. A comprehensive prototyping, testing, and evaluation effort was executed very early in the development phases.[3] Trade studies were conducted to select the configuration and materials to minimize the mass and operating temperatures, with the goal of keeping array temperatures within the qualification range of existing materials, while meeting the spacecraft power requirements over the mission. The thermal environments considered were not just those that arise from nominal operation in cruise and Mercury orbit, but also included those from anomalous direct-Sun pointing at Mercury perihelion (the point in Mercury's orbit closest to the Sun, i.e., ~0.3 AU). The structural substrates for the arrays use high-thermal-conductivity graphite/epoxy (Gr/Ep) composite face sheets over an aluminum honeycomb core to minimize mass. Both sides of the substrates are populated with solar cells; one side is fully populated with 5.5-mil-thick single-junction gallium arsenide (GaAs/Ge) cells. This side is used to generate power from launch until the spacecraft reaches a Sun distance of about 0.6 AU. The opposite side contains only 30% GaAs/Ge solar cells. The remaining 70% of that side contains optical solar reflectors, or mirrors (see Fig. 3). This side is used inside of 0.6 AU. At these close Sun distances, solar intensity is sufficient to produce adequate power using only the 30% area covered with the solar cells. The optical solar reflectors reflect the excess solar incidence to minimize panel temperatures. Nominal operating temperatures in the near-Sun environment are kept below 150°C. However, if the arrays are pointed directly at the Sun at 0.3 AU, temperatures can exceed 250°C.

The solar array materials and construction were first proven using a custom high-temperature infrared oven over the range of +300°C to –105°C. High-solar-intensity illumination tests at 11 Suns were then conducted at the GRC facility to verify the array power-generating capability.

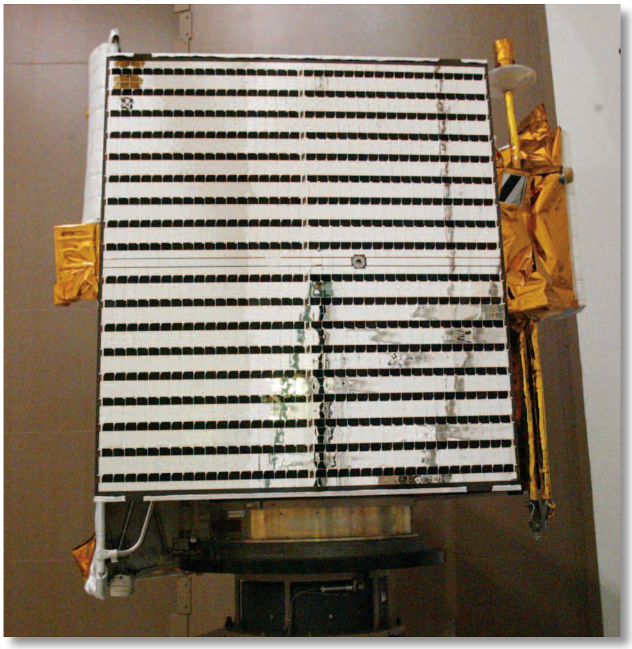

Figure 3. The MESSENGER high-temperature solar array with optical solar reflectors.

Fault Protection

The fault protection design of the MESSENGER spacecraft is driven by the need to maintain a safe thermal operating environment. If there is a pointing anomaly at Mercury, the amount of time the spacecraft can survive is very short. Therefore, maintaining a safe thermal operating environment primarily means assuring that the spacecraft attitude does not expose the spacecraft instruments and electronic components to direct solar illumination. (The spacecraft sunshade must be kept between the Sun and the rest of the spacecraft.) The system must also respond to other events that could mean potential loss of mission, such as losing contact with Earth for some period of time or having a battery charge below a critical value. The system can switch between redundant system elements and then “phone home” for further troubleshooting and correction. A key measure of the system performance was how quickly it could detect and act to protect the spacecraft from a fault that could otherwise lead to a loss of the mission.

Onboard fault protection functions are typically distributed among flight hardware, embedded software, and an autonomy engine that runs on one of the spacecraft processors. The autonomy engine consists of a suite of logical “if–then” rules, which evaluate onboard data against stored limits and execute stored command macros in response to rules that evaluate as “True.” These rules, the stored limits, and the command macros can be easily changed during flight without the need to recompile the processor application software. Examples of autonomy rule usage are to detect components that are not functioning properly and, in response, reconfigure the spacecraft to a fully operational state by switching to a redundant component, or if that cannot be achieved, demote the state of the spacecraft from operational mode to the “safe” (“phone home”) mode.

The autonomy engine used on MESSENGER was first developed for the APL-led NEAR mission. Lessons learned from NEAR led to the more capable autonomy engine design used for MESSENGER. One of the enhancements for MESSENGER was the ability to perform mathematical operations on the onboard data. For instance, MESSENGER has the ability to calculate the power consumption of a component by multiplying the input current and voltage, and it can take action if power consumption exceeds a predetermined limit. By contrast, NEAR autonomy rules evaluated only the input current to a component. Power consumption is more constant over variations in input voltage, whereas input current can change over a wide range. As a result, power consumption is a more reliable indicator of component health.

Another enhancement of the MESSENGER autonomy system was the ability to logically evaluate more arguments in the “IF” portion of the rule. That is, rules could be constructed as: IF (Condition A) AND (Condition B) OR (Condition C) . . . THEN (Command Macro Call). The previous implementation on NEAR could evaluate a maximum of only four conditions per rule. MESSENGER allowed evaluation of up to 32 conditions per rule.

While the MESSENGER autonomy engine overcame some of the previous limitations, the increased power of the engine came at the price of increased complexity. The number of possible paths made the system extremely difficult to analyze to ensure that rules were not in conflict and that the desired end state was achieved through every path. The only way to ensure proper implementation was to test all possible paths, resulting in a testing effort whose scope far exceeded the testing required on previous projects. The scope of the testing effort was not appreciated until after the engine and the rules were being formulated. The number of rules was ultimately descoped prior to launch to manage this complexity. MESSENGER launched with 208 rules and 164 command macros.

The lessons learned from the MESSENGER autonomy experience were applied to the New Horizons project, which strove to keep the number of rules to a minimum and to employ simpler rule constructions to avoid unmanageable complexity.[4]

NEW HORIZONS SYSTEMS ENGINEERING AND MANAGEMENT CHALLENGES

NASA had studied a mission to Pluto for many years, finally canceling all plans for a Pluto mission in late 2000 when the cost estimates exceeded available resources. However, many in the space community were convinced that such a mission should not be so expensive. Several unsolicited white papers, including one from APL, were submitted to NASA outlining concepts for missions at a cost of approximately $500 million. This convinced NASA to issue an AO, which led to the award of New Horizons to Dr. Stern and APL.

The APL proposal elaborated on the concept developed for the white paper; the experience of the staff with the operations concept developed by APL for the NASA CONTOUR mission was applied to the Pluto mission to help lower costs over a long operational phase (the 9.5-year cruise to reach Pluto). Several power-saving modifications to our existing electronics designs were identified to accommodate the limited power available from the government-provided radioisotope power source (RPS). Thus, the systems engineering practice of closely coupling programmatic elements and engineering implementation—classically a hallmark of the APL Space Department—was essential to the success of the mission development and execution.

The driving challenges for the New Horizons mission were both technical and programmatic:

- Spacecraft mass (largely driven by the extreme launch energy required)
- Certification of a new launch vehicle carrying a nuclear power source
- The integration of launch vehicle stages from competing launch providers
- The fixed power available from the nuclear power source
- The operations concept (long cruise period, science obtained on flyby, long round-trip light travel time)
- Risk management (the risk of implementing a Pluto mission was one of the reasons earlier attempts had failed)

Mass

The New Horizons mission was constrained in multiple ways, both technical and programmatic. Technically, the spacecraft mass was constrained by the extreme launch energy required for the Pluto-direct trajectory. This constraint required not only the usual discipline of the spacecraft development team to stay within the mass allocation, but also challenged the launch vehicle provider (Lockheed Martin) to maximize the launch vehicle performance.[5] (See Fig. 4.)

The spacecraft launch mass was 478 kg, less than half of the MESSENGER mass, with only 77 kg of fuel. The science payload was 33 kg. The design of the spacecraft electronics was baselined in the original white paper as a rebuild of existing proven APL designs. The few modifications made were driven by power constraints or long-life reliability considerations. The baselined spacecraft components and instruments were accommodated into the available launch mass with adequate margin throughout development. The high heritage (extensive previous flight experience) of the components provided confidence that the mass constraints could be met. The challenge was to minimize changes.

Launch Vehicles and Launch Approval

New Horizons was launched onto a direct trajectory to Pluto. The only mid-course corrections required are to correct for statistical errors. Still, the mission required the most powerful launch vehicle available (aside from the shuttle launch system), the two-stage Lockheed Martin Atlas V, and the launch energy required the use of a Boeing Star-48B third stage.

Atlas and Boeing at the time were competitors. Boeing was under contract to APL to provide the third stage as part of what Lockheed considered to be the payload to their Atlas V. However, a high degree of integration was required between the organizations to ensure this first-time interface would be compatible and successful, presenting a significant programmatic challenge. Additional complications were the requirements for launch vehicle certification by NASA; the Atlas V was a relatively new launch system at the time of the New Horizons launch. The specific configuration (5-m fairing with five solid-fuel strap-on boosters) had never flown before, and never had a Boeing third stage flown on the Atlas V. Additional requirements were imposed by the use of an RPS.

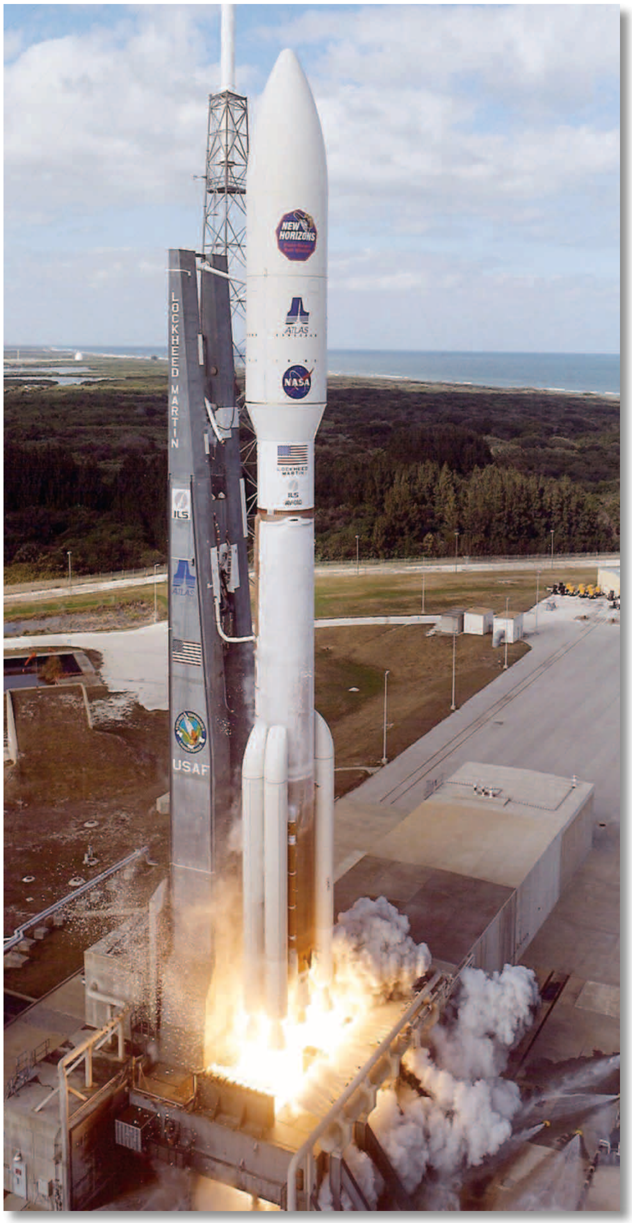

Figure 4. The New Horizons mission, whose design required careful management of spacecraft mass and the largest available launch vehicle (the Atlas V 551).

The approval for launching an RPS came only after compliance with two different regulations. The first is the National Environmental Policy Act of 1969 (as amended), and the second is defined by the National Security Council document NSC 25, which requires final approval for launch from the White House (typically the Office of Science and Technology Policy). Both regulations require a rigorous process of independent safety analyses and review. The analyses required a system approach, examining scenarios that ranged from launch accidents to radiation-induced health effects on the global population.

The previous RPS mission was the NASA Cassini mission to Saturn, launched in 1997. The launch approval process took 8 years for Cassini. New Horizons accomplished this in 4 years, largely because of the leadership and resources provided by NASA, Dr. Stern, and APL in working through an exhaustive, interdisciplinary process. APL drew on past experience supporting the Department of Energy's (DoE's) launch approval engineering activities to understand the critical elements of the process and to initiate action either using APL resources or coordinating with NASA and DoE to accomplish the analysis and gain the necessary approvals in time to meet the January 2006 launch.[6]

Power

The New Horizons and Mercury missions are at the opposite extremes of solar system exploration. Pluto is our most distant planet in the solar system. When the New Horizons spacecraft makes its closest approach to Pluto as it flies by in July 2015 (the spacecraft will not go into orbit around Pluto), Pluto will be ~34 AU from the Sun. Solar intensity is ~1000 times less at Pluto than at Earth. Generating electrical power from solar cells is therefore impractical; the area of the solar array would have to be 1000 times that of an array in Earth orbit to provide sufficient power. For this reason, New Horizons uses an RPS, specifically, a radioisotope thermal generator (RTG), which converts the heat from the radioactive decay of plutonium into electricity (see Fig. 5).

Another technical constraint is the limited power from the RTG. Because the electrical power is derived from the heat of plutonium decay, the output power peaks at the beginning of the mission and declines predictably with time. The usual system-level trade of mass for power that is available on photovoltaic (solar cell) spacecraft (by increasing solar array size in response to increased power demand from the spacecraft components) was not an option. Again, the extensive heritage of the baselined components provided confidence from the earliest stages of development that the power constraints could be met. And again, resistance to power-increasing changes was required. This constraint defined requirements not only for each subsystem, but also on the allowed operational modes of the spacecraft. At the time of the Pluto encounter (July 2015) the RTG is expected to produce 201.6 W. The spacecraft operating modes will be limited to less than 191.6 W (10 W of margin), as determined by the mission systems engineer.

The power constraint drove one of the few technology developments on the New Horizons spacecraft. A low-power digital receiver was developed for the spacecraft communications system, lowering the power requirement by more than half for this component compared with previous designs.[7] Like many other APL departments, the Space Department identifies areas where independent research and development can enable future tasks critical to sponsors. The Department also recognizes that these efforts must bring the technology to a level of readiness such that the development risk is mitigated once its use is committed to a critical task. These internal investments were successful in reducing the risk of implementing the receiver technology on New Horizons. The resulting power savings, along with other power-saving measures, such as the use of flash memory and a spacecraft thermal design that uses the dissipated heat from the spacecraft electronics to maintain a benign thermal environment over the course of the mission, enabled the execution of the mission with the only available RTG.

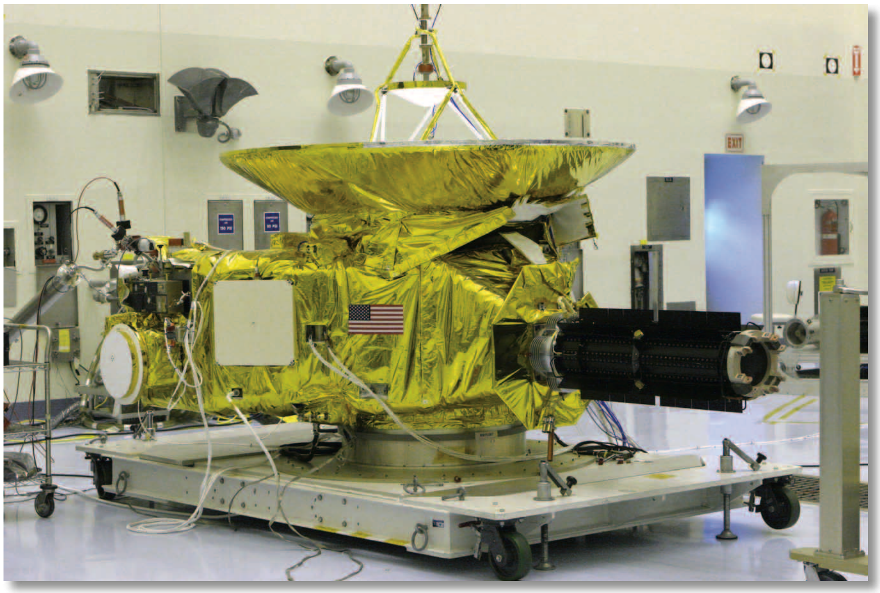

Figure 5. The New Horizons spacecraft is shown during final checkout at Kennedy Space Center. The RTG was essential to power the mission, but its use required significant analysis to meet the safety requirements of the launch approval process.

Operations Concept

The long mission life presented challenges to the spacecraft design, particularly the design of the onboard fault protection system. The long mission life also presents challenges to sustaining operations over an extended period; to minimize operations costs, an operations concept devised for use on the NASA CONTOUR mission was developed. This concept puts the spacecraft in a stable spinning attitude during long-duration, low-activity cruise periods. This minimizes onboard monitoring and processing and minimizes ground operations.

The spacecraft also operates in a three-axis-stabilized attitude for science operations during the Pluto system flyby. Thus our hands-on experience from the CONTOUR mission development directly influenced and enabled the low-cost approach to the New Horizons mission implementation.

The flyby nature of the mission also requires a different onboard fault-protection approach than an orbital mission such as MESSENGER. (Although MESSENGER completed multiple Mercury flybys prior to orbital insertion in 2011, the science from the flybys was not required for mission success. An orbital mission around Pluto was not feasible; the required onboard propulsion fuel would cause the spacecraft mass to exceed the launch vehicle capability.) The criticality of executing the proper sequence of spacecraft maneuvers and science instrument operation is exacerbated by the 9-h round-trip light time between Earth and Pluto at the encounter; this requires a higher degree of onboard spacecraft fault protection, but with a different set of goals. The goal of the MESSENGER fault protection system is to keep the spacecraft thermally safe. The orbital nature of its mission means science operations are tolerant of interruptions. The goal of the New Horizons onboard fault protection is to keep the science observation sequences executing during the encounter, even if the spacecraft should experience various anomalies. Redundant observations are also built into the sequences to provide some measure of robustness to interruption. In addition, the "one-shot" nature of the mission and the high-value science return (Pluto is the only "planet" not yet visited by a spacecraft from Earth) also resulted in more attention than usual to some multiple-failure scenarios. High-value scientific spacecraft are often designed to avoid only credible single-point failures. While addressing all multiple-point failures in a system design would result in an impractically large and heavy spacecraft, the New Horizons design did address some multiple-failure scenarios.

The spacecraft (though kept simple by design) resulted in more than 2 trillion combinations of operating modes into which the spacecraft could be commanded. The "art" of the systems engineering task was to develop a fault protection system that could protect the spacecraft from the most likely faults but that also could be tested. The resulting system for New Horizons incorporated (at launch) 126 rules that checked onboard telemetry for proper spacecraft operation and 132 command sequences that could be triggered to take corrective action if the rules identified a fault in the spacecraft operations. In addition to testing of each rule and command sequence, a set of 28 fault scenarios was crafted to test the full system response to potential faults and provide confidence that the system was sufficiently robust. During the first 4 years of flight, further system testing and experience in operations has led the team to make modest adjustments to the system. But, in general, the design developed prior to launch (and the general reliability of the spacecraft) has been demonstrated to serve the mission well.

Risk Management

The identification and management of risks was seen as an essential element in assuring the sponsor that the mission could be executed within available resources and schedule. A set of risks was identified as part of the proposal and updated each month throughout the program (this process continues during the flight phase and will not end until mission termination in 2017 or beyond). There are many risks at all levels of such a complex project. Many are identified by the engineering staff and are managed at the subsystem level. More significant risks and risks that cross system element boundaries are managed by the systems engineering staff and the project manager. Part of the management challenge is to ensure that the proper attention is paid to these risks at the proper level of the organization and to articulate these risks so as to assure that the proper resources are applied in their mitigation. This is especially important when the mitigation lies outside the direct control of the project. New Horizons had a number of risks of this type, as well as risks directly under the project's control. The openness of the Space Department allowed risks understood by the staff to be visible to the systems engineering and management team, with work on mitigation initiated early, before the risk could be realized. This visibility was also extended to the sponsor and to organizations not directly under either the project manager's or the sponsor's control.

The National Environmental Policy Act launch approval was the most significant risk and was outside the control of either the project or the sponsor. Articulation of that risk, with identification of a mitigation plan, was essential in getting all stakeholders to focus on the necessary tasks to meet the scheduled launch date. The launch vehicle certification and management of the interfaces was another element largely outside of the project's control. Again, by proactively identifying the risks and mitigations required and articulating them among the responsible agencies, the appropriate resources were committed to achieve success in time to meet the 2006 launch date.

CONCLUSIONS

The MESSENGER and New Horizons missions provide concrete examples where applying APL systems engineering attributes was key to making these critical contributions to critical challenges. A combination of technical expertise tempered with a practical approach to problem solving among small, tightly coupled teams, as well as the close coupling between our technical and programmatic disciplines, brought these missions to fruition, at low cost.

Although the staff expertise and organizational culture have served these missions well, the organization must continue to learn and improve. The Space Department created a systems engineering laboratory to perform studies of potential new missions to better facilitate the established culture of engineers and scientists working across their discipline boundaries. This laboratory has been used extensively in the past year to study new planetary missions in support of both APL-led teams and the community at large, including the National Research Council's survey of new planetary missions for the 2013–2023 time frame. Another example of this improvement was the shift in boundary between hardware-implemented fault protection and autonomy software implementation in response to differing requirements. To provide a better balance, the Department moved fault protection responsibility to a more formal systems engineering-focused part of the organization, while retaining the autonomy software elements in software-focused groups. These organizational changes provide a better alignment of skills and toolsets used for analysis, design, and testing. And these changes enhance the organization's ability to take on the next set of critical challenges.

ACKNOWLEDGMENTS: The ability of the Space Department staff to develop the missions described in this article is a testament to their skills in systems engineering. We acknowledge the culture that is able to balance technical requirements as well as cost and schedule constraints to achieve the challenges of these missions.

REFERENCES

[1] McAdams, J. V., Farquhar, R. F., and Yen, C. L., "Improvements in Trajectory Optimization for MESSENGER: The First Mercury Orbiter Mission," *Adv. Astronaut. Sci.* **109**(III), 2189–2203 (2002).

[2] Ercol, C. J., "MESSENGER Heritage: High-Temperature Technologies for Spacecraft to the Inner Solar System," in *Proc. AIAA Space Conf.*, Long Beach, CA, paper AIAA 2007-6188 (2007).

[3] Ercol, C. J., Jenkins, J. E., Dakermanji, G., Santo, A. G., and Mason, L. S., "Prototype Solar Panel Development and Testing for a Mercury Orbiter Spacecraft," in *Proc. 35th Intersociety Energy Conversion Engineering Conf.*, Las Vegas, NV, paper AIAA-2000-2881 (2000).

[4] Moore, R. C., "Safing and Fault Protection for the MESSENGER Mission to Mercury," in *Proc. 21st Digital Avionics Systems Conf. (DASC)*, Irvine, CA, paper 9.A.4 (2002).

[5] Kusnierkiewicz, D. Y., Hersman, C. B., Fountain, G. H., Vernon, S. R., and Stratton, J. M., "System Engineering Challenges on the New Horizons Project," in *Proc. International Aerospace Congress*, Valencia, Spain, paper IAC-06-D1.5.03 (2006).

[6] Chang, Y., "Aerospace Nuclear Safety at APL: 1997–2006," *Johns Hopkins APL Tech. Dig.* **27**(3), 253–260 (2007).

[7] Haskins, C. B., and Millard, W. P., "X-Band Digital Receiver for the New Horizons Spacecraft," in *Proc. 2004 IEEE Aerospace Conf.*, Big Sky, Montana, pp. 1479–1488 (2004).

The Authors

David Y. Kusnierkiewicz

Glen H. Fountain

David Y. Kusnierkiewicz joined the APL Space Department in 1983 and was the Mission Systems Engineer for the NASA Thermosphere, Ionosphere, Mesosphere Energetics and Dynamics (TIMED) and New Horizons missions. He has been the Chief Engineer of the Space Department since 2004, and he teaches in The Johns Hopkins University Engineering for Professionals program. **Glen H. Fountain** has been in the APL Space Department since 1966. He has held numerous positions during his career at APL, including spacecraft Guidance and Control Engineer, Systems Engineer, Instrument Development Group Supervisor, Engineering Branch Supervisor, and Project Manager for the New Horizons mission to Pluto, for which he received the American Institute of Aeronautics and Astronautics Von Braun Award for Outstanding Space Program Management (2007). In addition to being Project Manager, Mr. Fountain also led the process to obtain approval from the U.S. government to launch the New Horizons spacecraft with a radioactive power source, a 4-year process that presented the largest risk to meeting the launch schedule. For further information on the work reported here, contact David Kusnierkiewicz. His e-mail address is david.kusnierkiewicz@jhuapl.edu.

The *Johns Hopkins APL Technical Digest* can be accessed electronically at **www.jhuapl.edu/techdigest**.