RISK MANAGEMENT: A PRACTICAL DESIGN TOOL FOR SPACE SYSTEMS AND TECHNOLOGY DEVELOPMENT

ERIC A. SILK[†]
Thermal Engineering Technology Development Group, NASA Goddard Space Flight Center,
Greenbelt, MD 20771

PAUL H. DASH[§]
Economic & Business Analysis Group, Booz Allen Hamilton,
5220 Pacific Concourse Drive, Los Angeles, CA 90045

1 ABSTRACT

Over the past two decades, risk management and risk analysis have emerged throughout the business community in the United States (US) as prominent planning and development strategies used to mitigate risk of failure and ensure a high return on investment (ROI) for business endeavors (financial and otherwise). They are generic tools that can be applied to any business regardless of the sector (i.e., government, university, private) and have been used by the Federal government in the form of institutional practices aimed at maximizing the probability of success in business activities. One US Federal agency that incorporates risk management and analysis techniques into business and/or engineering activities is the National Aeronautics and Space Administration (NASA). The present work is a discussion on mission, spacecraft and instrument design (as well as technology development) and the role of risk management, analysis and mitigation as a fundamental tool in the design process.

2 INTRODUCTION AND BACKGROUND

The primary objective of every spacecraft program at NASA is mission success. Mission success is measured relative to the mission's technical goals as dictated by the principal investigator. Techniques to ensure mission success (i.e., mission assurance) are used in spacecraft development at each assembly level (i.e., spacecraft, instrument, subsystem, and component). Engineering design on each of these levels is subject to four criteria: technical performance, size, cost and risk of failure [1]. Each of these criteria are applied to spacecraft design from concept to flight and are often used to tailor engineering decision making that eventually leads to a flight ready product. While these criteria are presented as individual design

Submitted to AIAA Journal of Spacecraft and Rockets *Submitted for review on September ?, 2007*
† Corresponding Author
§ Senior Business Consultant
Email address: Eric.A.Silk@nasa.gov

parameters, close examination of the design process shows that they are not mutually exclusive, but intricately coupled.

Technical performance may be assessed in terms that are easily quantifiable, however, the criteria of size and cost are slightly more pervasive. In spacecraft design, volume and mass are used to quantify the metric of size. Spacecraft and/or instruments that have a large volume require a larger payload and launch vehicle. A larger launch vehicle also requires more fuel in order to ensure transit to deployment altitude outside the earth's atmosphere. In addition, more mass also implies an increase in fuel is needed at launch to provide thrust levels commensurate with the launch vehicle's total mass. An increase in the projected fuel consumption for the launch vehicle implies an increase in comprehensive program costs. Thus, from a program perspective, cost corresponds directly with size. Since cost projections for proposed missions are a continually increasing concern in the context of the US national budget, mission success may be considered a function of two criteria: technical achievement of mission goals and cost effectiveness associated with the attainment of these goals. Cost effective designs for spacecraft systems must aim to meet technical performance requirements while designing size and mass efficient spacecraft that meet the mission mass budget and launch vehicle size constraints. Risk management and analysis have become useful tools in meeting this challenge.

3 RISK MANAGEMENT AND SPACECRAFT DESIGN

The topic of risk analysis often takes the form of reliability analysis in engineering applications. However, for the present discussion, the general term of risk analysis shall be used henceforth. Risk may be considered the possibility of exposure to an adverse consequence given certain actions. In regards to space flight applications this could be a safety accident, a budget overrun, a slip in schedule, or failure to achieve mission success due to selection of a particular design for use [2,3]. Risk analysis pertains to the quantification of uncertainty associated with certain adverse events (i.e., the chances of an undesirable event occurring) [2]. Risk management deals with decision making under conditions of uncertainty while using quantified measures of uncertainty in the decision making process [2,3]. Inherent to risk management theory is the definition of utility. Under conditions of uncertainty, the utility of a particular decision may be defined as the consequence of each possible outcome associated with the decision. The goal of risk

management is to investigate the trades between different conveniences and consequences (i.e., utilities) for each possible outcome given a situation involving uncertainty [2].

Risk management, as applied to spacecraft design, investigates the utilities associated with specific mission and system designs on all levels. This includes identification, analysis, planning, tracking, controlling and documenting (as well as communicating) risks and the corrective measures developed to address them [3]. The three primary tools used in the implementation of risk management are Failure Modes Effects Analysis (FMEA), Fault Tree Analysis (FTA), and risk mitigation. FMEA is used to identify mission failure modes and associated utilities for each system design element. FMEA is also used to categorize failure modes according to severity. FTA is instituted to specify credible ways that an undesired event can occur [3]. Upon determination of mission endangering utilities pertaining to desired design options, risk mitigation techniques are applied to the design to increase the probability of mission success (i.e., decrease the risk associated with the design selection process and/or the design leading to the actual mission). Application of methodologies that mitigate risk of failure have a direct effect upon mission costs. Mitigation techniques are often incorporated into spacecraft design and assembly through the use of spaceflight hardware and procedures from legacy space flight programs, redundancy of mission critical components as well as technology and manufacturing validation of system components. Successful flight legacy programs with an established performance record serve as a basis for expected performance on future missions that use similar flight system components. Integration and test procedures borrowed from such programs aid in the reduction of human error (and associated impacts) during integration at each of the assembly levels. This further reduces the probability of increasing program costs through new and extensive engineering efforts to ensure in-flight performance of components. System and component level redundancy also is a technique that has been used to mitigate mission risk. Redundancy of critical system components (e.g., lasers, sensors, detectors, thermal control hardware, etc.) increases the probability of mission success if failure of a primary component were to occur. However, system redundancy often leads to higher program costs. As such, many modern spacecraft programs either opt for selective redundancy (i.e., redundancy applied to a few critical items) or a single string approach (i.e., no system redundancy designed into system critical space flight components). A primary factor in the determination of risk of failure associated with a spacecraft assembly is the risk of failed performance associated with the individual

components comprised in the assembly. Full technology validation of component level items is critical to mission success and aids in the mitigation of risk at each of the spacecraft and instrument assembly levels. Furthermore, it decreases the need for additional validation efforts during assembly phases that may also require additional funding. Nonetheless, component level validation is best addressed in the technology development stage of the space flight hardware in question.

4 TECHNOLOGY DEVELOPMENT

As one of the vanguards of human science and technology, NASA is always eager to promote new concepts and ideas that have the potential to grow and aid in future flight programs through mission enabling technologies. The approach used by NASA to establish new technologies while also mitigating in-flight risk of failure is to subject the component in question to a regiment of tests designed to validate successful in-flight performance and decrease the probability of failure. This goal is achieved through a technology development and maturation plan designed around the technology rating level (TRL) system and lifetime testing. The TRL system (shown in Table 1) has rankings from one to nine and is aimed at developing technologies from the breadboard phase up through flight readiness. Upon achieving TRL 8, technologies are acknowledged as being viable for use on actual performance based missions. TRL 9 is validation of successful flight performance on an actual mission. The TRL system is applied to all technologies actively developed through NASA's technology development programs: Small Business Innovative Research (SBIR), Small Business Technology Transfer (STTR), Internal Research and Development (IRAD), and New Millennium programs.

Each of the development levels in the TRL system is assigned a relevant environment for testing. These environments are based on ground (TRLs 1-6), micro-gravity (TRLs 7-9), and space (TRLs 7-9) platforms. Ground based testing may consist of testing in a thermal vacuum chamber to simulate pressure and temperature conditions in space. Such facilities are easily accessible in the government and private sector. However, from both a technical and logistics standpoint, the more challenging of these environments to simulate and test in is micro-gravity. Test apparatus that simulate the effects of micro-gravity are not limited to space based platforms. NASA's drop towers (located at NASA Glenn Research Center) and reduced gravity aircraft have been used in technology development efforts to characterize

component performance in micro-gravity. The NASA Glenn drop towers can provide a maximum of 3.3 seconds of micro-gravity whereas the parabolic flight profiles associated with reduced gravity aircraft testing provide approximately 22 seconds of micro-gravity during a single flight parabola. Under these approaches, the time constant associated with micro-gravity conditions is significantly shorter than the amount of time required to reach system equilibrium for many experiments. Thus, other methodologies are required for sustained micro-gravity testing. In previous years, the Space Shuttles' payload bays have been used to provide a sustained micro-gravity test platform for emerging space technologies (i.e., the Hitchhiker and Get Away Special (GAS) programs which are currently non-active). However, the emergence of the International Space Station (ISS) and delivery of components to it via the Space Shuttles significantly reduced the availability of Shuttle payload bay space for technology development efforts, hence reducing the number of technologies satisfying mid-level TRL requirements. In addition, the Space Shuttle Columbia disaster further limited payload bay access for technology development programs. Today, microgravity requirements are satisfied for growing technologies through space flight on missions specifically designed and created for technology validation such as the New Millennium program and the Department of Defense's Tactical Microsatellite Experiment (TacSat) missions. Nonetheless, such missions have limited availability of space and relatively high mission costs, thereby limiting the number of technologies validated through these missions.

An additional technique used to mitigate risk that may be considered complementary to the TRL system is lifetime testing. Lifetime testing is not explicitly addressed in the TRL system, however, it is highly pertinent to space flight programs seeking to mitigate risk (especially those that are not particularly sensitive to gravitational effects). The primary objective of the TRL system is to validate new technologies as flight proven in a relevant mission environment. The primary objective of lifetime testing is to demonstrate component and/or system performance as well as the determination of possible performance degradation to components that are subjected to extensive use. This applies to subsystems (i.e., electrical, mechanical and thermal) on all assembly levels. The afore-mentioned technical goals used to gauge mission success are based on temporal specifications. The temporal metric for mission success is the expected mission lifetime. Longer missions (≥ 5 years) entail more durable components which increases costs through material selection and engineering design time. Thus, mission lifetime is a driver for system design

as well as the selection of components and machinery for use on space flight missions. The amount of risk associated with the use of a component often incorporates continuous lifetime performance (either through ground based lifetime testing or legacy flight systems) relative to the desired mission life. Furthermore, achievement of TRL 9 does not negate or diminish the importance of lifetime testing and performance. The larger the amount of time a component or system has operated within desired performance specifications on orbit, the more reliable it is considered.

6 CONCLUSIONS

For several years, NASA has been instrumental in the creation and validation of new technologies that later matriculated to the civilian sector and revolutionized the American way of life. The basis for the successful development of these technologies are risk management (based on quantified measures of uncertainty), risk analysis and mitigation techniques that are rooted in the institutional practices of NASA. The risk mitigation practices and procedures detailed in this work are examples of common risk prevention techniques borrowed from the private sector, as well as institutional practices created and refined in-house through years of successful engineering efforts. Today these practices are part of NASA culture. As technical complexity for mission programs and Federal budget constraints increase, risk management, analysis, and mitigation techniques that complement the engineering process are expected to become more important and refined in aiding the success of NASA's future flight missions.

DISCLAIMER

The ideas and opinions expressed in this document are solely those of the authors' and do not represent official NASA policy.

ACKNOWLEDGEMENTS

Eric Silk was supported by the Thermal Engineering Branch and the Technology Transfer office at the NASA Goddard Space Flight Center. Paul Dash was supported by the Economic & Business Analysis group of Booz Allen Hamilton in Los Angeles, CA. Special thanks also to Dan Butler of NASA Goddard Space Flight Center's Thermal Engineering Branch for his insights.

REFERENCES

[1] Silk, E.A., and Creel, R., 2007, "Technology Development for Lunar Thermal Applications and the Next Generation of Space Exploration," *Journal of Aerospace Engineering,* Vol. 221, No. 2, pp. 305-309

[2] Singpurwalla, N.D., 2006, "Reliability and Risk: A Bayesian Perspective," John Wiley & Sons, Ltd., Washington, D.C.

[3] NASA Goddard Space Flight Center Office of Mission Success/Code 170, 2005, "Goddard Procedural Requirements: Directive No. GPR7120.4A," Goddard Space Flight Center, Greenbelt, MD

List of Tables

Table 1.

TRL Level	Definition	Validation Environment
1	Basic principles observed and reported.	Ground based laboratory
2	Technology concept and/or application formulated.	Ground based laboratory
3	Analytical and experimental critical function and/or characteristic proof-of concept.	Ground based laboratory
4	Component and/or breadboard validation in laboratory environment.	Ground based laboratory
5	Component and/or breadboard validation in a relevant environment.	i) Microgravity platform (airborne or ground). ii) Vacuum environment ($\leq 10^{-6}$ Torr)
6	System/subsystem model or prototype demonstration in a relevant environment (ground or space).	i) Microgravity platform (airborne or ground). ii) Vacuum environment ($\leq 10^{-6}$ Torr)
7	System prototype demonstration in an operational environment.	i) Microgravity platform (space)
8	Actual system completed and "flight qualified" through test and demonstration (ground or space).	i) Microgravity platform (airborne or space).
9	Actual system "flight proven" through successful mission operations.	i) Microgravity platform (space)

Table 1. Technology Readiness Level Definitions