ON SPACE EXPLORATION AND HUMAN ERROR
A paper on reliability and safety

David A. Maluf and Yuri O. Gawdiak
National Aeronautics and Space Administration
David.A.Maluf@nasa.gov, Yuri.O.Gawdiak@nasa.gov

David G. Bell
Research Institute for Advanced Computer Science
DBell@arc.nasa.gov

Abstract

NASA space exploration should largely address a problem class in reliability and risk management stemming primarily from human error, system risk and multi-objective trade-off analysis, by conducting research into system complexity, risk characterization and modeling, and system reasoning. In general, in every mission we can distinguish risk in three possible ways: a) known-known, b) known-unknown, and c) unknown-unknown. It is probable almost certain that space exploration will partially experience similar known or unknown risks embedded in the Apollo missions, Shuttle or Station unless something alters how NASA will perceive and manage safety and reliability.

1. Introduction

Current and future NASA Exploration goals include missions with the most difficult, dangerous, and dynamic operations in history, ranging from Earth orbit operations to planetary and universe exploration. These missions, by their nature, push the limits of human, technological, and theoretical knowledge boundaries.

NASA continues to push technology limits with its missions, and exploration is not an exception. Increased system functionality often results in increased implementation complexity, making both success and affordability much harder to achieve. Moreover, it is accepted that not all human risks can be mitigated during design: Human reliability in systems cannot be verified with full coverage and components will fail or degrade, operators will make mistakes, and operating environments are uncertain. In addition, the state of the system and its environment may dynamically increase control complexity or decrease reaction times such that traditional control means are inadequate. Development of critical technologies that provide system resiliency will enable future systems to adapt and recover from these unanticipated problems. Significant improvements in critical technologies will be required to reduce risk in future NASA missions.

This paper will underline the scope and importance of human reliability in NASA space exploration for now and for the future.

2. Successes and Failures

NASA's record of mission success is strong. However, the ever-increasing complexity of NASA missions will significantly challenge NASA's ability to assure mission success.

With all of its success, NASA has had failures that have cost billions of dollars, have lost opportunity for scientific advancement, and more tragically have resulted in the loss of human life. Notable failures include the first manned Apollo flight in 1967 which resulted in four fatalities, the Space Shuttle Columbia in 2003 which resulted in seven fatalities, the Space Shuttle Challenger launch in 1986 which resulted in seven fatalities, and the Mars Climate Orbiter and Polar Lander missions in 1999 which cost more than $1.5B. In the period of 1986 to 2001, the top ten NASA failures cost around $9.6B, with half of that cost due to the loss of the Space Shuttle Challenger. NASA is not alone in experiencing such failures during

that time period, with estimates of total U.S. space mission failures costing $18.6B and worldwide space mission failures costing $31.1B. Rates of failure for U.S. launch vehicles (NASA, DoD and commercial) have been estimated to be 7.6% for the period of 1985 to 1999. The costs of failure are high, and the rates of failure are not appreciably improving.

The need for improving risk management is recommended as the highest priority by many NASA internal and independent studies and commissions. The Faster Better Cheaper Final Task report recommends that missions develop and maintain "Programmatic and Mission Risk Signatures," making risks and risk countermeasures visible to all inside and outside the project (FBC p.4). The NIAT report (Enhancing Mission Success) recommends that NASA "Improve and enhance NASA and contractor knowledge and ability to identify, assess, mitigate, and track risk through the definition of success criteria, acceptable risk, utilization of existing and new tools, and proper policy and guidance" (NIAT-7, p.42). The NIAT cites 31 separate recommendations supporting enhanced risk management among the recent mishap reports.

NASA has taken major steps toward managing its risks. Presently, recent major mishaps considered by the CAIB, NIAT and others (e.g., Mars Climate Orbiter, Lewis Spacecraft, Mars Polar Lander, Wide-Field Infrared Explorer, and the V-22 rotorcraft), and various strategic agency analyses (e.g. Shuttle Independent Assessment Team, the Faster, Better, Cheaper Task Report, and the U.S.A.F. Broad Area Review of 1999) have identified the critical need for NASA and the U.S. aerospace industry to significantly retool its engineering processes and capabilities.

3. Space exploration and human error

In every mission we can distinguish risk in three possible ways: a) known-known -- we know the risk and have retired it, b) known-unknown -- we know that there is a risk and the risk is modeled and c) unknown-unknown -- we don't even know there is a risk. Exploration is about diving in the unknown-unknown.

3.1 Risk mitigation for the probably future

Mishap analyses continue to highlight humans as contributing factors to mishaps. For example, poor knowledge management contributed to the Ariane 5 and Space Shuttle SSME repair mishaps. Hubble and other case studies such as Challenger and Columbia also point to management and cultural issues as key factors in mishaps. Some argue that humans are always involved in mishaps and assert that the causes of mishaps are frequently, if not almost always, rooted in the organization—its culture, management, and structure. However, it is insufficient to focus exclusively on social and organizational factors; how these relate systematically to technology development, deployment, and use is also important.

Analyses of recent major mishaps (e.g., Mars Climate Orbiter, Mars Polar Lander, and Wide-Field Infrared Explorer), various strategic agency analyses (e.g., NASA Integrated Action Team, Shuttle Independent Assessment Team), and various case studies have consistently identified knowledge management and humans as contributing causes to mishaps.

An Aerospace study examined nearly 4000 launches from 1957. Based on the analysis results, this paper recommends enhancements for launch vehicles, including avionics redundancy, software and integrated system testing. Human-in-the-loop processes, software function and propulsion and flight control subsystem failures ranked high as initiators of mishaps. The mishap data presented in a Boeing report indicates that loss of control in flight is the leading cause of fatal accidents and controlled flight into the terrain is the second leading cause in commercial airline accidents. Contributing factors in these accidents included software errors, component failures, improper human-machine interactions (poor training), operator error on-board or on the ground (sometimes due to an uninformed operator) and unanticipated operating environments. In fact, flight crews expressed the desire for real-time, onboard integrated diagnostics that provide "answers not just clues" to the causes of anomalous conditions occurring during flight. Nonintegrated caution warnings are not sufficient because the crew is responsible for cognitive integration that takes precious minutes and could mean the difference between life and death.

The identification of technology is a major part of a solution set that will have significant impact on mitigating the risk in future NASA missions. In general, failures constantly suffer poor requirements specification and system verification, and rigid operations and control systems have been inferred as major causes of mission mishaps. **Current technologies are not optimal for carrying out effective risk mitigation strategies as they lack significant capability to assess system condition or to validate system performance. System robustness,**

redundancy and capability for rapid recovery are currently inadequate.

It is *probable almost certain* that exploration will partially experience similar known or unknown risks embedded in the Apollo missions, Shuttle or Station unless something alters how the enterprise will perceive and manage safety and reliability.

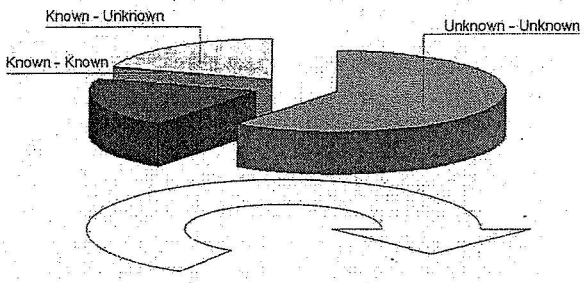

Figure 1: In every mission we can distinguish risk in three possible ways: a) known-known -- we know the risk and have retired it, b) known-unknown -- we know that there is a risk and the risk is modeled and c) unknown-unknown -- we don't even know there is a risk. Exploration is about diving in the unknown-unknown.

In order to establish technology development priorities for risk mitigation in space exploration future missions, the focus should be on three main goals (type of risks) including 1) determination of the major problem classes involved in NASA missions and such mastering the known risks in mission design 2) determination of precursors of risk (latencies) and 3) identification of processes to capture and model new risk. Figure 1 illustrates the lifecycle of risk. Exploration (unknown-unknown) brings new experience where new risk is modeled and understood (known-unknown). Capabilities can then transform and retire the risk (known-known).

NASA space exploration should largely address a problem class in reliability and risk management stemming primarily from human error, system risk and multi-objective trade-off analysis, by conducting research into system complexity, risk characterization and modeling, and system reasoning. The state of the art and foundation in this category appears to be well established, but the resulting mishaps and catastrophes demonstrate and tell us otherwise. There are clearly things missing or not addressed in today's state of the art approach, either in technology or organizations. Development activity will have to support risk analysis, design robustness, failure modeling, and system trade-offs throughout the entire lifecycle of the enterprise, with particular emphasis on early-phase capabilities. Today we can only imagine the state of the art of safety and mission assurance. Although we do utilize modern tools and techniques to analyze our systems and make risk decisions, these present methods have significant limitations.

3.2 The need to manage risk for sustainable exploration

Various studies have also highlighted the need to continuously manage risk throughout the life cycle. Studies also uncovered the fact that risk analysis should not only be conducted linearly but recursively as well. This means that changes in the later phases of a program require revalidation of earlier life cycle phases, such as requirements, design, etc., in order to fully quantify potential risk exposure.

NASA has to invest in a variety of defenses that constitute reliability for exploration. Such defenses include physical barriers, personal protective equipment, procedure design, training, and the like. A variety of partially redundant defenses typically intervene between a hazard and the losses that would result if that hazard occurred. It is only when all the defenses are unfortunately aligned and therefore penetrated that a mishap occurs.

There are four latent conditions critical to the space exploration: the distributed nature of work, the heterogeneous nature of work, data overload, and the presence of advanced automation and decision support information technologies. These four elements in part define the complexity of work that gives rise to a variety of risk situations.

In general, when work is distributed across space and time among multiple people, certain latent conditions necessarily exist that may lead to future mishaps. These include information sharing, coordination, communication, procedures, training, and knowledge capture and reuse. Information sharing may be absent, incomplete, incorrect, or not done in a timely manner. Coordination activities may be disorganized, untimely, missing, or unnecessarily difficult for a particular organizational structure. Poor communication practices, inappropriate initial framing of the interaction, poor training, and poor procedure design may lead to poor information sharing and coordination, which may directly lead to mishaps, or indirectly create 'deeper' latent conditions of mistrust or inappropriate group norms among members of the organization. Distributed work also requires distributed knowledge; therefore, poor knowledge capture and lack of reuse are issues as well.

A second latent condition is the heterogeneity of work. The complexity of NASA missions demands the integration of heterogeneous skills and knowledge from a diverse workforce. For example, power systems engineering, structural engineering, orbital mechanics, astrophysics, computer architecture, data handling, and flight dynamics are just some of the technical disciplines involved in building and operating spacecraft (to say nothing of the difference between engineering and management). These disciplines constitute "micro-cultures" with their own norms, jargon, and styles of interaction that may be incompatible and lead to misunderstandings and failure.

A third latent condition is the proliferation of data and information. The greater quantity and specialization of work, as well as the greater quantity and sophistication of information technologies described below, leads to a serious data overload problem for human practitioners. Information technologies themselves are often developed with the goal of reducing data overload by providing tools for information fusion, decision support and automation. While often successful at one level, at another level such technologies add to the complexity of work.

Automation and decision support information technologies are another necessary facet of NASA missions that is the basis for a number of latent conditions. Such information technologies play into this analysis in a number of ways. Automated systems perform many functions in the operational environment. Engineering design and analysis relies on any number of software packages. Training systems are often implemented as interactive computer-based exercises. Simulations are used for engineering design and training and can and should be used as an aid to develop requisite imagination. Of particular interest is the use of model-based simulations to support vehicle or system design. A key problem that faces NASA is the proliferation of models and tools for high-fidelity but isolated component models and the associated lack of an integrating framework so that models can be used together effectively. Questions of what model fidelity is good enough for different kinds of decision making and how integrated models can support more effective team and organizational problem solving are critical issues.

3.3 Managing the known-unknown or risk mitigation

The intersection of distributed work, heterogeneous work, data overload, and technology is useful to consider explicitly in the context of "poor knowledge management." A study on why knowledge management is difficult found four major factors: (1) Ignorance (people don't know that what they know is useful or know that somebody else knows something useful), (2) No "absorptive capacity" (people don't have the time, money and management resources to explore and reuse others' knowledge), (3) Lack of preexisting relationships (knowledge flows best between people who know, respect, and like each other), and (4) Lack of motivation (people don't perceive value added). A fifth commonly cited factor is also clumsy knowledge management technology; yet, as many authors have pointed out, the hard problems are really always with "the people."

Space exploration should address the development and utilization of a variety of tools, processes, and capabilities, largely built around a framework of information technology. Means for better modeling and characterization of risk (both human and historical - design/ops phase) and its relationship to complexity and known or potential anomalies, visualization (understanding) of risk and risk profiles, integration methods, particularly those for integrating highly disparate models, and tools enabling the utilization of risk models in active design trades are examples of capabilities instantiated in IT.

Space exploration investments in new technologies to support full lifecycle, integrated risk management is critical for successful missions. This will support the development of integrated risk management tools and risk profiling capabilities instantiated in multiple categories:

Category 1 – Development of *tools for identifying, assessing and trading risks* before and during formulation; improvements in risk management from the outset will yield benefits throughout the mission lifecycle.

Category 2 – Development of *safety and risk-related systems analysis tools*, combines two thrusts, addressing a) how risk profiles can be maintained and utilized throughout the full lifecycle, and b) how system evolution affects designs.

Category 3 – Development of methods and tools that constitute a human learning 'feedback' loop. Their goal is to *improve our understanding of the factors that contribute to aerospace accidents* and to develop ways to use that experience to improve designs.

Space exploration should focus on short-term and long-term objectives. One key short-term objective is to realize the risk characterization of a mission/system model with full breadth and with depth significant enough to demonstrate the utility of a true risk-based design paradigm – that is, to characterize the system risk sufficiently and early enough to be fully traded in the design phase, along with and against other typical system attributes, and to fully define the benefits thereof.

The long-term goal is to support the development and deployment of an integrated full-lifecycle capability that is infused into all infrastructures supporting the enterprise missions. This capability would improve our understanding of risk and risk precursors for all mission/system types and the relationship between risk and complexity, provide for full and complete modeling of risk at the system and subsystem levels at all phases, and significantly improve our ability to reliably design, build, and operate Agency missions. In addition, the ability to fully understand risks and the effectiveness of risk mitigation (such as testing), can also help to optimize the retirement of risk and, indirectly, to reduce the cost and development time of missions.

4. A unique opportunity

New exploration missions have now a renewed opportunity to address risk with novel capabilities in early phase design when compared to Shuttle and Station; key developments supporting other phases, particularly operations, will be fostered due to their importance to key customers and because of the valuable insight that it provides regarding management of the transition between phases and continuing model maturity. As the new exploration projects progresses, the emphasis will move toward later parts of the lifecycle and the transition between phases that are necessary to maintain model integrity; the goal will be to eventually demonstrate a capability applicable to full-lifecycle design and operations.

1. Model Based Risk Management involves methods and tools to model accurate cause and precursor identification, communication, and learning, including taxonomies and frameworks to enable comprehensive, comparative analyses and trending in mishap and anomaly reporting data for exploration missions, and information organization, analysis and visualization tools to facilitate and manage distributed processes.

2. Risk Assessment involves the principal research and component-level developments supporting new methods of risk characterization and visualization, risk modeling, probabilistic assessment capabilities, and development of relevant historical and causal data supporting risk assessment and management. In addition, the scope will extend further into the mission lifecycle in order to ensure compatibility with subsequent phases and avoid the phase-transition problems that have plagued other programs.

5. References

[1] Chaisson, E.(1995). The Hubble wars: Astrophysics meets astropolitics in the two-billion-dollar struggle over the Hubble Space Telescope. Harper Perennial.

[2] Davenport, T. (1994). Saving IT's soul: Human-centered information management. Harvard Business Review, March-April 1994, 121.

[3] Dorner, D. (1996, English translation). The logic of failure: Recognizing and avoiding error in complex situations. Addison-Wesley.

[4] Hollnagel, E. (1993). Human reliability analysis: Context and control. Academic Press.
Jones, P. M. (1999). Human error and its amelioration. In A. Sage and W. B. Rouse (Eds.), Handbook of systems engineering and management. Wiley.

[5] Leveson, N. (1995). Safeware: system safety and computers. Addison-Wesley.

[6] O'Dell, C. and Grayson, C. J. (1998). If only we knew what we know: The transfer of internal knowledge and best practices. Free Press.

[7] Perrow, C.(1984). Normal accidents: Living with high-risk technologies. Basic Books.

[8] Reason, J. (1990). Human error. Cambridge University Press.
[9] Reason, J. (1997). Managing the risks of organizational accidents. Ashgate Publishing.

[10] Senders, J. W. and Moray, N. P. (1991). Human error: *Cause, prediction, and reduction.* Lawrence Erlbaum Associates.

[11] Star, S. L. (1995). The politics of formal representations: Wizards, gurus, and organizational complexity. In S. L. Star (Ed.), Ecologies of knowledge: Work and politics in science and technology. SUNY Press. *Chang/Aerospace study (AIAA Journal of Spacecraft & Rockets)*

[12] Statistical Summary of Commercial Jet Airplane Accidents (Worldwide Operations 1959-2000); StatSum@PSS.Boeing.com

[13] ARC Mission Cause Classification ECS L1 final report, Pantonin et al., 2001 (to be released), and http://www.defenselink.mil/news/Apr2001/t04052001_t405mv22.html

[14] Safeware: System Safety & Computers, Leveson, N., Addison Wesley, 4th ed., 2002, Chapter 4.

[15] DoD SW Engineering Science and Technology Summit Report

[16] Engineering for Complex Systems, L1 Program Plan Article Title: U.S. NTSB Officially Pins United 585 Crash On 737 Rudder , By SEAN BRODERICK, 05-Jun-2001 3:33 PM U.S. EDT

[17] www. aviationnow.com

[18] Article Title: Upset Events, Wake Vortices At Center of Flight 587 Probe, By FRANCES

[19] Fiorino, 4/22/2002 www. aviationnow.com
Article Title: NTSB Wants Revamped Maintenance Procedures In Alaska Crash Aftermath, By
Sean Broderick , 02-Oct-2001 3:30 PM U.S. EDT www. aviationnow.com

[20] Article Title: A330 Overwater Flameout Raises ETOPS Issues, By FRANCES FIORINO, 9/01, and http://seattlep-i.nwsource.com/business/boeing10.shtml www. aviationnow.com

[21] AIAA Model Based System Level Health Management for Reusable Launch Vehicles, Clancy, 9/2000.

[22] DIALOG(R)File 471:New York Times, Late Edition - Final ED, COL 01, P 7 , Sunday October 14 2001
Dragonfly, Burrough, B., HarperCollins Pub., 1998 (a) part three, pg 341, (b) part one, pg. 3.
[23] The Black Box, Editor MacPherson, M., William Morrow Pub. 1988, pg. 162.
http://www.nist.gov/public_affairs/releases/n02-07.htm

[24] Arthur Anderson Technology Market Survey Final Report, 2001, http://nmp-techval-reports.jpl.nasa.gov/DS1/Remote_Integrated_Report.pdf