Cognitive Flexible Risk Implementation Model and Management

Arnold Baldwin
Houston Space Professionals Chapter
National Society of Black Engineers
Houston, TX, USA
abaldwin@nsbe-hsp.org

Jeneene Suttle
Space Special Interest Group
National Society of Black Engineers
Huntsville, AL, USA
jsuttle@nsbe-space.org

Abstract - *This paper will attempt to explore the emerging trends in risk implementation and risk management. Cognitive risk involves the ability to formulate risk concepts simultaneously while continuously thinking and developing new ideas. Flexible risk involves the ability to adjust and adapt a risk posture in light of potential of loss resulting from a given action, activity and or inaction. No matter how much physical science and technology is involved in complex systems, no system is purely or solely physical or technical. Further, no known system is purely scientific or technical in its operation or management. Research on and the modeling of complex systems usually relies heavily on the consideration of technological variables and processes, thus typically failing to consider the contributions of individual psychological, organizational and contextual factors.*

Keywords: Risk management, multi-destination, Moon, Mars, Asteroid, NSBE Visions for Human Space Flight Working Group.

1 Introduction

The Space Special Interest Group of the National Society of Black Engineers has commissioned a *Visions for Human Space Flight Working Group* to investigate technical challenges surrounding NASA human space flight and to identify an alternative path for the direction of United States human space flight. Research conducted by working group participants and documented in this paper represents volunteer labor executed on behalf of NSBE, a 501(c)3 nonprofit headquartered in Alexandria, VA. NSBE coordinates the inputs of aerospace industry experts to propose innovative solutions to complex technical challenges facing the United States. This paper, in coordination with six other Working Group papers, collectively encompasses the product of the Working Group's efforts. Recommendations, results, and conclusions in this paper do not reflect NASA policy or programmatic decisions.

1.1 Complex Systems

The world has witnessed a remarkable revolution as it relates to technical advances, perhaps most notably in human spaceflight systems that have been achieved and are now being proposed. As technology has advanced, the technical systems employed have grown in complexity and size. This increases the attention that must be paid to risk management of complex systems (CS). Many failures have occurred because of inadequate oversight of CS. CS catastrophic events include the British Petroleum oil rig explosion, NASA Mars Rover failures, the Constellation Program's cancellation and numerous others in the private and public sectors. The events occurred because of the failure to recognize them as CS. Complex systems require risk assessments that include psychological, social, organizational and political processes, in addition to those typical of traditional engineering practices. Some may question how political processes may be considered CS. However, political processes play an enormous role in dealing with risks in the public sector and in many private sector instances. Risk assessment shapes design, construction and management of infrastructure systems solutions, therefore attention needs to be paid to its implementation.

2 Risk Control

The idea behind innovative risk implementation is a matter of looking at a dual focus: the focus of Risk and Risk Control. Taking risk and exercising control is both innovative and critical to understanding a Programs or Projects risk appetite and risk tolerance. The innovative idea behind Risk and Risk Control is looking at the interaction of the two as part of determining risk appetite. Proportionately more time is likely to be spent on risk taking at a strategic level than at an operational level. When a Program or Project is at the operational level the focus is more likely to be on the exercise of control of the risks.

3 Risk Appetite, Risk Tolerance, and Performance

Risk appetite and risk tolerance are inextricably linked to program performance over time. Risk appetite refers to the level of risk that the organization is willing to pursue or accept. Risk tolerance, by comparison, refers to the level of risk that the organization can absorb without incurring failures or other performance losses. In a risk-averse culture, risk appetite is substantially below risk tolerance. Typically such a culture will impose a high degree of rigidity in its processes to control risk to the desired level. This may result in higher costs and decreased performance. However, in a risk-prone culture, risk appetite may approach or even exceed risk tolerance. In such a case, if risk appetite is slightly below risk tolerance, then significant cost savings or performance gains may be realized. But if risk tolerance is exceeded, catastrophic failures may occur.

It is clear that Programs and Projects have to take risks in order to succeed. However, the big question that all Programs and Projects should ask themselves is what does successful performance look like? Where is their risk appetite in relation to their risk tolerance? Both risk appetite and risk tolerance can be expected to vary throughout the life cycle of a Program or Project, so these are quantities that must be controlled actively.

Risk tolerance can generally be expressed in terms of absolutes. For instance, a propulsive loss of X% will result in the spacecraft being unable to achieve its design delta-v objective. Risk appetite defines what risks the Program or Project is willing to undertake that could potentially impact this risk tolerance – for instance risks induced by mass, cost, personnel, or training decisions. A project may pursue a 10% reduction in cost by reducing the number of personnel assigned to the propulsion subsystem, which may result in a less efficient design with a corresponding propulsive loss of n%. In order to ensure that n% is less than X%, it is incumbent upon the Program and Projects to define all relevant parts of the risk management system and to ensure that risk management throughout the organization maintains a risk appetite within the boundaries of risk tolerance.

The Multi-Destination Human Space Flight Program Office faces the difficult challenge of developing a family of spacecraft within a ten-year period under a $300M annual budget capable of launching expeditions (many of which are in parallel with one another) to the Moon, Mars, and Near Earth Asteroids. [10] Managing risk appetite and risk tolerance is a multidimensional problem as traditional methods of reducing risk in one area are likely to exceed risk tolerance in another.

4 The Assessment and Calculation of Risk

Risks are calculated to prioritize the design of the most likely and potentially damaging hazards and to evaluate the adequacy of the design. Risk assessments shape the design, therefore great attention should be paid to how it is done. There are five critical systems that strongly depend on the following factors; 1) The inherent complexity of the system and the environment in which it exists and operates; 2) The models utilized to represent the system; that is how the system, its environment and its complexity are represented; 3) If the models provide equal weight to the technical, individual human, organizational and socio-political variables determining the operation, and the failure modes of the system; for example, whether certain variables are emphasized or privileged over others and when the representation of the system is fundamentally biased or flawed; 4) A direct result of factor 3, the number and kinds of terms included in determining the probability, or the probabilities, of failure of the system; 5) How the consequences of the failure of the system are also represented and determined.

A “System” consists of a complex set of technical processes and variables that interact strongly with a complex set of individual human organizational and socio-political processes and variables. Technical and individual variables of the system can only be distinguished from one another with great difficulty. The variables are so strongly coupled it is almost impossible to determine where one typically begins and the others end.

Modeling a complex system is inherently interdisciplinary. This means that determinations of the probabilities of the system failures are also inherently interdisciplinary. The assessment of risks associated with the complex systems is inherently interdisciplinary as well.

Modeling and risk assessment of complex systems have not been as interdisciplinary as they need to be. As a result, a basic and fundamental error underlies the vast majority of risk assessments. This error is known as the Error of the Third Kind or the Type Three Error (E3) [6].

E3 is defined as the ‘probability of solving the ‘wrong’ problem precisely. E3 pertains to how problems are defined or formulated initially. By taking technical, individual human, organizational and socio-political variables equally into account, E3 can be expressed on a quantitative basis. An interdisciplinary approach to modeling complex systems allows us to formulate and determine the E3s. Organizations that regulate risk assessments to individuals with narrow technocratic expertise will inevitably commit E3s. Incorporating multiple perspectives and being alert to discrepancies

between models and reality can help organizations deal with risk in a realistic and proficient way.

Defining the problem as primarily an "engineering problem" is almost always a major E3. Problem definition is critical in designing, operating, maintaining and managing critical CS. The human, organizational and institutional causes of complex systems are termed "extrinsic." The categories of uncertainties traditionally addressed by engineers – natural or inherent and those associated with parametric, state and analytical model uncertainties are termed "intrinsic." Neglecting extrinsic factors – which are actually fundamental to system performance – can cause expected risks to be under predicted by factors of 100 or more. These findings are consistent with a large body of research that highlights the role of "extrinsic" factors in large-scale system failures. [2], [8], [11], [13]

Traditional engineering analyses and processes also result in inappropriate strategies for managing risk. These analyses and processes readily lend themselves to commit E3s as the result of thinking that overemphasizes improving "things" such as system components, rather than addressing "process" and "people" factors that produce risk and the consequences of risk. [4], [3], [12]

5 Risk Management Proposal for Managing Programs and Projects

To cover the spectrum of risk when dealing with CS it is important to develop a holistic approach that incorporates analytic models that model relationships among factors and processes taking place at four levels of risk analysis: technical, physical systems, organizational processes and practices, and the broader societal context.

Physical systems and their components is the domain of traditional engineering risk analysis and management. Human elements of organizations traditionally studied by psychologists include individual differences, personality, and training. Scholars specializing in the sociology of organizations, management science, organizational communication, and related fields traditionally study organizational attributes and processes. This includes a range of factors including organizational structure, culture, management and problem-identification, and problem-solving strategies. However, in order to incorporate the broader societal factors that affect both organizational processes and physical elements of CS a more macro-level approach is required. The macro-level includes factors such as governance, laws and regulatory regimes, and social, demographic and economic forces that must be taken into account in CS risk and vulnerability analyses. Physical systems and their components fail to address the critically important issues associated with the consequences of failure, particularly those associated with rescue and recovery resilience. Individual differences and organizational and social sciences enable a more holistic assessment of risks and the management alternatives to reduce the likelihoods of failures and consequences contributing to CS risks.

This approach provides the philosophy that CS vulnerability can only be achieved through analysis of interactions within and across the four areas previously discussed. Managing risks is a multidimensional problem that must be addressed through collaborative research and educational activities that cross and transcend disciplinary boundaries. When implementing a risk management plan for Programs and Projects that require concurrent engineering it is critical to ensure that all team members have a basic understanding of risk management, understand that a comprehensive risk management strategy should encompass not just technical risks but physical system risks, organizational process risks, and societal risks. If risk management is part of the conceptual phase of a program/project and the technical, physical system, organizational process, and societal risks are factored the Programs/Projects will have a higher rate of success by understanding the known risks and the ability to deal with the unknown risks that are inherent in CS.

6 Risk Management Staffing and Training

The Multi-Destination Human Space Flight Program Office employs a staff of ten FTE risk managers, five at the Program Office level and two within each Project Office. [10] One Program Office position is a full-time position that serves as the Lead Risk Manager. The additional four FTE in the Program Office are respectively experts in technical risk, physical system risk, organizational process risk, and societal risk, but all also possess general risk training. The four FTE may be held by four full-time individuals or distributed among part time allocations as determined by the Program. The two risk management FTE within each Project Office may represent a mixture of specialist and generalist training, but will include expertise in all four risk types. All risk management personnel will possess necessary expertise for both risk management practice and training. Risk management personnel working in conjunction with program training instructors will provide annual risk management training to all project personnel and additional targeted training on a position-specific basis.

7 Risk Tracking and Ownership

All risks are tracked. However, a particular approach is recommended for this program. It is typical in NASA and DOD systems to express risk in terms of likelihood and consequence. We believe this approach may only provide part of the risk position because it is very difficult to

accurately represent the likelihood of risks in human spaceflight. Even for technical risks, there is often not enough flight experience in appropriate environments to have statistically valid values for mean times between failures or other probabilistic approaches to quantify likelihood. Non-technical risks such as political risks are even less predictable. Literature review also reveals significant concerns with risk matrices. [1], [5] Instead, risks for this program are tracked by type, threat, and control.

Risk type refers to the previously mentioned assessment that a risk management strategy cannot be effective if limited to only technical risks. Risks are organized into type T, P, O, and S risks, as indicated below:

> T – Technical – Related to design, engineering, manufacturing, technological processes, and test procedures – generally applied at the component or individual item level
>
> P – Physical System – Resulting from the integration of multiple technical components
>
> O – Organizational Process – Related to organizational structure, culture, management and problem-identification, and problem-solving strategies
>
> S – Societal – Related to governance, laws and regulatory regimes, and social, demographic and economic forces

In addition, each risk is assigned a threat level, numbering 0 through 5 as described below. This is somewhat comparable to the risk consequence used in traditional risk matrices.

> 0 – Non-Credible – A non-credible risk is one that has been proposed but has been determined to not be capable of occurring under the current configuration
>
> 1 – Trivial – A trivial risk has an impact on the system that is so small it cannot be effectively measured or noticed.
>
> 2 – Minimal – A minimal risk has an impact on the system that is noticed, but compensation can be achieved within existing margins
>
> 3 – Reactive – A reactive risk has a significant impact on the system and can only be contained with significant use of resources that may require replanning or adjustment
>
> 4 – Inhibiting – An inhibiting risk has a severe impact on the system and cannot be fully contained; some intended aspect of the system is lost
>
> 5 – Catastrophic – A catastrophic risk has a non-recoverable impact on the system and results in loss of crew, spacecraft, or major mission objective

Finally, risks are tracked with respect to the level of control exerted against the threat:

> A – Suppressed – Existing measures have effectively prevented the occurrence of a risk or have negated the significance of its impact
>
> B – Limited – Existing measures reduce the likelihood of occurrence or provide some mitigation against the threat of the risk but do not provide complete protection
>
> C – Uncontrolled – No measures are in place to prevent the occurrence of the risk

As an example, a MMOD impact to an EVA helmet might carry a risk of T5B, meaning it is a technical risk that could result in loss of crew and is controlled with limited measures that do not completely protect the astronaut against its occurrence or severity.

Every risk is assigned an owner. In the case of a technical risk, this may be a subsystem engineer. The general idea is to assign ownership at the lowest organizational level possible, to the person most directly empowered to affect the risk.

Each risk owner is responsible for implementing corrective action, including where necessary negotiating design refinements with other subsystems or spacecraft, to reduce the risk threat and/or increase risk control. The risk owner is also responsible for identifying direct and indirect linkages to other risks.

Each risk owner is also assigned a risk manager, one of the two risk managers in his or her Project Office in the case of project staff, or one of the five risk managers in the Program Office in the case of program staff. Through the use of appropriate information management tools, the risk owner must keep the risk manager up to date with the real time status of all assigned risks.

During a monthly Program Risk Management Forum the risk managers will prioritize risks and recommend elevation of any risks as warranted. To aid in their prioritization, they may choose to invite subject matter experts, program or project office personnel, or other

external experts as needed. This forum may be a multi-day meeting depending on the scope of risks to be discussed. Risks that require Project Office or Program Office intervention may be elevated to the Program Management Forum. They may also bring risks forward to the Program Systems Engineering Forum, applicable Communities of Practice, the Training Forum, or Test and Verification Forum [10] depending on the nature of the involved risks. At minimum all risks with a combined threat-control level of 3B or greater are reviewed at the quarterly Program Technology Review Forum. [10]

8 Risk Management by Milestone

Major program milestones will lead to shifts of focus for the Program as the component spacecraft move from concepts to reality. While this will lead to shifts of emphasis related to some risks, others will remain constant.

Throughout all phases of the program one of the key families of risks to monitor is the family of risks impacting cost, schedule, and budget. This family of risks includes risks from all four types.

Criticism of the Constellation program was largely centered on cost, particularly cost-induced schedule delays [7] that were feared to be so great that they would render any attempted return to the Moon meaningless because the development program would stretch to absurd levels. In an attempt to forge a recommendation, the Augustine Commission weighed various alternative strategies for human spaceflight – Mars First, Moon First, Flexible Path [7] but such comparisons ultimately hold little value because all of these strategies assumed the same acquisition model that made Constellation unaffordable. Any human spaceflight endeavor beyond the current program (ISS, Orion, SLS, plus Commercial Crew and Cargo) under current acquisition models requires a budget in excess of that which can be reasonably expected from Congress. The only solution is to change the acquisition model, which carries inherent risks that must be managed.

The NASA X-38 program is well known for its attempt to demonstrate a NASA capability to achieve dramatic cost reductions. The spirit of the X-38 approach is at the heart of the recommendation for this Program – a set of small, high expertise, in-house teams performing hands-on spacecraft development. Because program cost is primarily tied to the labor cost of the workforce, the key to dramatic cost reduction is dramatic workforce reduction – any given activity must be completed with significantly fewer personnel. In the case of this program it implies a workforce of approximately 1006 total full time equivalent people, distributed across a Program Office and five Project Offices. Each Project Office is a slightly smaller team than the X-38 team. Risk management will play a pivotal role in maintaining this reduced cost without sacrificing quality or schedule and protecting crew safety and mission objectives.

Political risks are another important family of risks that will achieve special attention throughout the program life cycle. While many of these are type S (Society) risks, there are risks of other types with political impact. They may relate to internal Agency organizations, Congressional or White House considerations, commercial industry, or international politics.

In addition to these, and perhaps a few other families of risk that will maintain near-constant focus throughout the life of the Program, there are other risks that will be more closely tied to specific phases of the Program lifecycle. Certain phases will place emphasis on specific broad categories of risks.

During the Concept Development Phase, the primary focus of risk management will be the prevention of Errors of the Third Kind. This phase is where the configuration of the architecture is developed. Although this phase concludes with the Mission Concept Review (MCR), it is a MCR that follows extensive testing including a 180-day mission and subsystem testing with medium fidelity hardware [9] – something that was never attempted by the Constellation Program, despite it having proceeded well beyond MCR. It will be particularly important to control risks that could push the architecture in a direction that would leave it fundamentally unable to satisfy its objectives. Also, because risks will help shape test activity, it will also be important to ensure the risks are sufficiently developed to drive the proper selection of test activities.

The System Development Phase includes an 860-day mission and subsystem testing with high fidelity hardware. [9] It is important to emerge from this phase with a complete vehicle design that can be produced within the available resources and does not have obvious or hidden design flaws. During this phase the primary risk management focus will be on protecting the integrity of the design. The majority of related risks will be type T and P (technical and physical system risks), but organizational process and societal risks will also have implications for the designs of the various vehicles and overall architecture.

The Production Phase includes manufacture, integration, and qualification and acceptance testing [9] and results in the delivery of flight-ready spacecraft to Kennedy Space Center. During this phase, risk management will prioritize those risks related to production quality and testing effectiveness. Type P risks will likely dominate this phase, but all three other risks are likely to continue receive additional attention.

During the Operations Phase, manufacture of follow-on flight units will continue, but from this phase forward

hardware and crew will begin to be launched into space. Therefore, safety of flight operations will be the dominant risk focus. Because safety of flight involves so many disparate aspects, all four types of risks will be of high importance. It is worth reflecting that the Apollo 1 fire, *Challenger* explosion, and *Columbia* accident all experienced the occurrence of non-technical risks that were contributing causes to their accidents.

The Termination Phase involves the archival of Program data and disposition of Program hardware [9] and while it might be tempting to conclude that the risk management function has terminated by this time, there is actually a very important risk management priority during this phase. Here, it is critical to future programs to leverage final Program resources to position the Agency for follow-on activity. Thus, priority will be given to risks that impact how the Agency leverages the resources of this Program for the benefit of future programs.

9 Conclusions

Researchers and decision makers exhibit a tendency to focus exclusively on the risks of accepting a false hypothesis regarding the true value of a variable. However, many fail to take into account the risk of rejecting a true hypothesis about the true value of a variable. Thus, the risks used as part of the analysis, are incorrect because key variables were omitted. This can be a methodological problem, which goes under the name of specification error or omitted variables bias. Models can produce precise calculations of the value of a risk that are nonetheless meaningless due to the model being incomplete. Risk management systems must be designed such that errors may be detected and corrected. This requires the broad input and willingness to reassess models, in light of the unexpected while proceeding forward with the design, test and manufacture of components.

Acknowledgment

The author would like to acknowledge the work of other members of the NSBE Visions for Human Space Flight Working Group and their contributions to an integrated rationale for human space exploration and development. The author would also like to thank all NASA civil servants and contractors who contributed to the Constellation Program, AES Program, and any other exploration design study or team.

References

[1] Anthony Cox, “What’s Wrong with Risk Matrices?”, Risk Analysis, Vol. 28, pp. 497-512, 2008.

[2] Clarke, L. and Short, J. (1993) Social Organization and Risk: Some Current Controversies. Annual Review of Sociology 19: 375-399.

[3] Farber, D.A., Bea, R.G., Roberts, K., Wenk, E. and Inkabi, K. (2007) Reinventing Flood Control. Tulane Law Review 81 (4): 1085 – 1127.

[4] Gehman, H.W. Jr. et al (2003) Columbia Accident Investigation Report, Vols. 6, Washington DC: Government Printing Office.

[5] Michael Power, “The Risk Management of Nothing,” Accounting, Organizations, and Society, Vol. 34, No. 6-7, pp. 849-855, August-October 2009.

[6] Mitroff, I.I and Linstone, H. (1992) The Unbounded Mind. New York: Oxford University Press.

[7] Norman Augustine, *Review of US Human Spaceflight Plans Committee*, White House Office of Science and Technology Policy, October 2009.

[8] Perrow, C. (1984) Normal Accidents: Living with High Risk Technologies. New York: Basic Books.

[9] Robert Howard, “A Systems Engineering Approach for a Multi-Destination Human Space Flight Architecture,” Proc. 2014 NSBE Aerospace Systems Conference, Los Angeles, CA, January 22-25, 2014.

[10] Robert Howard, “Program Organization of a Multi-Destination Human Space Flight Architecture,” Proc. 2014 NSBE Aerospace Systems Conference, Los Angeles, CA, January 22-25, 2014.

[11] Roberts, K.H. (1990) Some Characteristics of One Type of High Reliability Organization. Organization Science 1 (2): 160-176.

[12] Shirvastava, P. (1987) Bhopal: Anatomy of a Crisis. Cambridge, MA: Ballinger.

[13] Vaughan, D. (1996) The Challenger Launch Decision: Risky Technology, Culture, and Deviance. Chicago, IL: University of Chicago Press.