2003-01-2572

Reducing the risk of human space missions with INTEGRITY

Harry W. Jones
NASA Ames Research Center

Robin L. Dillon-Merrill
McDonough School of Business, Georgetown University

Terry O. Tri and Donald L. Henninger
NASA Johnson Space Center

ABSTRACT

The INTEGRITY Program will design and operate a test bed facility to help prepare for future beyond-LEO missions. The purpose of INTEGRITY is to enable future missions by developing, testing, and demonstrating advanced human space systems. INTEGRITY will also implement and validate advanced management techniques including risk analysis and mitigation. One important way INTEGRITY will help enable future missions is by reducing their risk. A risk analysis of human space missions is important in defining the steps that INTEGRITY should take to mitigate risk.

This paper describes how a Probabilistic Risk Assessment (PRA) of human space missions will help support the planning and development of INTEGRITY to maximize its benefits to future missions. PRA is a systematic methodology to decompose the system into subsystems and components, to quantify the failure risk as a function of the design elements and their corresponding probability of failure. PRA provides a quantitative estimate of the probability of failure of the system, including an assessment and display of the degree of uncertainty surrounding the probability. PRA provides a basis for understanding the impacts of decisions that affect safety, reliability, performance, and cost. Risks with both high probability and high impact are identified as top priority. The PRA of human missions beyond Earth orbit will help indicate how the risk of future human space missions can be reduced by integrating and testing systems in INTEGRITY.

INTRODUCTION

If human exploration is to once again go beyond low Earth orbit, there is a great deal of scientific research that needs to be accomplished soon. The performance of both the technical systems and the human astronauts in such a difficult environment are highly uncertain, and the risks to the spacecraft and to the astronauts are substantial. The INTEGRITY program will provide a ground test bed capable of accurately simulating all elements involved in beyond-LEO human missions. (INTEGRITY is a contraction of INTEGRated Human Exploration Mission Simulation FacilITY.) The primary focus of INTEGRITY is to integrate and evaluate technologies that enable missions beyond Low Earth Orbit (LEO). In addition, the program will develop and validate new management and engineering techniques that are critically needed in planning future space missions including computer-based design, cost control, and risk analysis methods. There is also a key education, outreach and public involvement component to the program. Some of the major areas that will require test and demonstration in INTEGRITY are habitat systems design and integration, environmental monitoring and control, advanced life support, crew selection and performance, cost control, risk mitigation, and mission operations and control.

The first task of the INTEGRITY program is the planning, advocacy, and development of INTEGRITY itself. The program is needed to provide critical research to support potential missions beyond LEO, and INTEGRITY must be scoped and designed to make the most cost-effective contribution to these future human missions. The problem is that there will always be more areas to study and problems to resolve than there is funding available. The implementation of INTEGRITY must be guided by the analysis of anticipated human missions, and the key to the success of the INTEGRITY program will be to focus its resources to have the greatest possible impact on reducing the risks associated with these missions.

In order to optimize the budget resources of the INTEGRITY program to have the greatest impact on reducing the failure risks of future missions, a program-level probabilistic risk analysis (PRA) is needed. PRA is a method to produce quantitative estimates of the risks

associated with complex systems, and quantitative estimates are necessary when budgetary prioritization is required (i.e., when we cannot have everything we want). Creating this probabilistic risk model of the system will allow the consideration of multiple risk factors, including technical risks such as safety and performance and management risks such as cost and schedule.

The INTEGRITY program can play a key role at this time in setting up a risk assessment methodology that can be continued by a specific project team as mission planning begins. Risk analysis is required for major NASA programs and projects, and it must be started in the earliest stages of planning.

Risk analysis can begin with limited data and then be refined as more information becomes available, and a PRA is the best approach to use when little statistical data is available. This is because the focus of the PRA is to decompose the system into subsystems and components to quantify the failure risk as a function of the design elements and their corresponding probability of failure. There can be a great deal of flexibility in the level of decomposition, and the appropriate level is determined by the level of detail available in the design. As the design matures, and more detail is available, the PRA can be refined without altering the basic structure of the analysis. Also, PRA is the best method for handling uncertainties. The model can be developed using expert assessments of uncertainties and then updated when statistical test data become available. Finally, a PRA can provide the structure for analyzing how human and managerial errors can contribute to mission failure.

INTEGRITY can begin now to develop a useful preliminary PRA. The PRA will follow the approach that has been developed by researchers and consultants and adopted by NASA for current missions (both crewed and uncrewed). INTEGRITY can use the results of the mission risk analysis in planning and advocacy.

The goal of INTEGRITY is to reduce the risk of future human missions beyond LEO. The emphasis will be on those high priority risks that INTEGRITY testing can reduce. Some elements of a long-duration human planetary mission have higher risk than others and some are easier than others to test and demonstrate in INTEGRITY. The PRA will provide a valuable tool for allocating resources among the different efforts to minimize the mission risk.

The paper includes the following sections:

- Qualitative versus quantitative risk assessment
- Performing a PRA
- Mission risks INTEGRITY can reduce
- PRA illustration
- Conclusion

QUALTITATIVE VERSUS QUANITATIVE RISK ASSESSMENT

A risk is the possibility that an undesired outcome occurs, and risks are generally defined by two components: the magnitude (or severity) of an undesired consequence and the likelihood of that occurrence.

NASA has traditionally done qualitative risk assessment using Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) without quantitative statistics. In a qualitative risk assessment, both the severity and probability of the negative consequences are described verbally, for example as high, medium, or low.

The results of a qualitative risk assessment can be shown in a two-dimensional matrix categorized by the severity and probability of consequences, such as Table 1 below. The highest priority risks are those with high probability and high severity, in the upper right corner of the matrix.

Table 1. Risk matrix.

		Severity		
		Low	Medium	High
Probability	high		2nd highest	Highest priority
	medium			2nd highest
	low	Lowest priority		

A qualitative assessment is appropriate as a first screening to identify the highest versus the lowest risks. But when resources are constrained and a more complete prioritization is needed, its usefulness is limited. For example, which is of greater concern: a medium probability-high severity problem or a high probability-medium severity problem? In recent years, NASA has emphasized more quantitative risk approaches. However, a qualitative risk assessment could be useful as a preliminary risk screening step for a PRA.

PRA is a method to produce quantitative estimates of the risks associated with complex systems. The systems initially examined with PRA were primarily engineering systems, but as the PRA methodology has matured, its applications have expanded. The essential part of the analysis is the identification of the most likely failure scenarios and the major sources of uncertainty. In order to analyze the system and identify the failure modes, a PRA relies on other engineering and risk analysis tools such as FMEA, FTA, and statistical analysis. The PRA

model should be comprehensive and useful for evaluating the risks from concept definition through design, development, operation, and decommissioning.

In PRA, the magnitude of an adverse consequence is expressed numerically, for instance as the number of hours or dollars lost, and the likelihood of its occurrence is expressed as a probability. With these data, decisions can be made based on the expected value of damage. The risk, however, is not simply the probability times the consequence, but is the whole set of scenarios defined by a risk curve.

The risk curve plots the decreasing probability of exceeding some severity value as a function of the increasing severity, where the probability of a scenario is graphed on y-axis against the corresponding consequence severity on the x-axis. The uncertainty corresponding to the scenario can be indicated by the width of the risk curve.

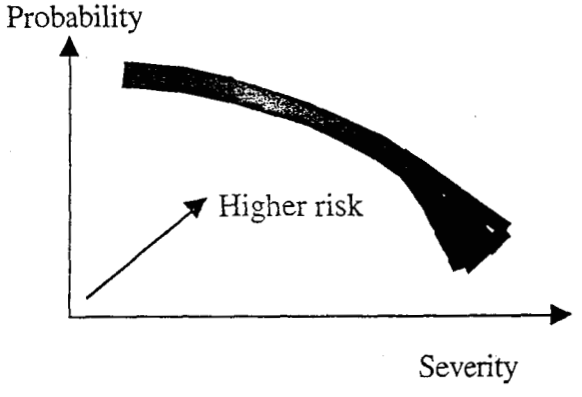

Figure 1. Risk curve.

PERFORMING A PRA

The general steps in a PRA are:

- Consider a system (technical, human, etc.) that can fail, sometimes catastrophically.
- Analyze it to identify the initiating events, the failure modes, the external events that can affect it and the human and managerial errors that contribute to its failure. [1]
- Compute the probability of failure as a function of the performance of different components or parts.
- Identify the possible ways to reinforce the system or prevent failure from happening.
- Prioritize the risks and mitigation actions.
- Perform sensitivity analysis on assumptions.

The first three steps provide the decision maker with a set of triplets that identify all possible scenarios, the probability of that scenario, and the consequences or evaluation measure of that scenario. [2] After completing the last step, the result is a ranked list of scenarios that can serve as a basis for the allocation of resources toward the improvement of safety and the reduction of risk. If we know the probabilities and consequences of all the potential failures, we can compute their risk values and plot the risk curve.

The remainder of this section provides more detailed discussion on identifying the initiating events and failure modes and computing the probability of failure.

IDENTIFY THE INITIATING EVENTS AND FAILURE MODES - PRA must consider both internal and external failure initiating events. Internal initiating events may include hardware failures or operator errors that occur in normal operation. External initiating events are those due to abnormal operating conditions such as an extreme radiation environment or those originating outside the system such as a terrorist event.

The event scenarios and failure modes must be developed using logic tools. Inductive tools start with initiating causes of failure and develop the subsequent events and consequences; tools include Event Tree Analysis (ETA), Event Sequence Diagrams (ESD), FMEA, and Reliability Block Diagrams (RBD). Deductive tools first assume a particular negative consequence and then identify possible causes; tools include FTA and Master Logic Diagrams (MLD). In addition, PRA studies sometimes require Human Reliability Analysis (HRA) to model human error and Common-Cause Failure (CCF) analysis to consider the effect of multiple internal dependencies.

For each initiating event and its possible end states, we construct a risk scenario using event trees and event sequence diagrams. Both representations start at the initiating event and progress through a series of alternate happenings called pivotal events, until the various end states are reached. For the planned PRA of human missions beyond LEO, at this preliminary phase, we will rely primarily on event sequence diagrams.

The pivotal events are those that either allow or prevent the initiating event from propagating to cause the undesired end state. Pivotal events include the effects of safety systems, crew interventions, and coincident timing. The favorable or unfavorable outcome of each pivotal event is usually modeled using Fault Tree Analysis. A fault tree includes the failure of the pivotal event, a logic network (AND and OR gates) of intermediate failures that can cause the failure of the pivotal event, and basic events. Basic events are the lowest level modeled events. Basic events are failures that ultimately cause the pivotal event to occur. The fault trees are simplified using Boolean logic to identify the cut sets and then quantified to yield the failure probability of the pivotal event.

Identifying initiating events, pivotal events, and basic events requires investigating a reasonably well-defined system, including analyzing the hardware, operating procedures, software, and environmental risks. The PRA should be started in Phase A, preliminary analysis, and updated and maintained over the life-time of the project as the systems are further specified. As the INTEGRITY program progresses the hardware, procedures, software, and environment become better defined.

COMPUTING THE PROBABILITY OF FAILURE - In some cases, the probability of an event is well known from past data. If adequate failure data is lacking, probabilistic failure models can be developed using inductive logic tools like FMEA and reliability block diagrams (RBD) or deductive logic tools like FTA. As INTEGRITY progresses more test data will become available that can be used to refine the model.

MISSION RISKS INTEGRITY CAN REDUCE

Since the crewed mission PRA that will be used to guide INTEGRITY will be performed during the preliminary analysis and early concept definition of a future human space mission, exact mission specifications and statistical failure data does not yet exist. Instead of a detailed PRA of the lowest-level hardware components as described above, the PRA for INTEGRITY should focus on the high-level crewed mission components. The failure probability data can be estimated from knowledge of past systems and can examine generic failure modes. At least initially, much of the PRA data will come from expert assessments.

PRA is considered necessary during concept definition, regardless of the incomplete design and failure information. The cost, performance, and risk of a system are largely determined during concept definition. PRA in early project phases gives useful risk information that can be used to select more robust system alternatives and to plan further risk mitigation. PRA is actually the most suitable approach for low probability, high severity events where few statistical data are available, because if the events are possible but rare and the sample size is small, then the event may not appear in a statistical data sample.

The objective of having INTEGRITY perform the PRA of a human space mission is to identify and prioritize the risks of human space missions beyond LEO, and especially to define the risks that INTEGRITY can mitigate. Although the PRA must include all the major risks of a human mission, it will specifically consider those risks that can be investigated and mitigated using a ground test bed. The result of the PRA will be a description of both the general mission risks and the specific risks that INTEGRITY can reduce, including the relative importance of the risks to the overall mission.

Since we want to include all the significant risks that INTEGRITY can help mitigate, we will develop an inclusive list of undesirable end states. Murphy's law is, "Anything that can go wrong, will go wrong." This is too negative, but anything that can go wrong, might go wrong.

A human space mission is a project, and all projects have cost, schedule, and performance objectives and thus have cost, schedule, and performance risks. Performance objectives include both delivering hardware and providing operational system performance. The most important aspect of performance is safety, and safety risk is the most significant risk. Achieving the safety, cost, schedule, performance, and operations objectives is a project responsibility, but there are risks external to the project, such as unavailable resources or problems with partners and customers. The risks outside project control are usually called program risks. The above mentioned risk categories are often used. [3] [4] [5]

Table 2 shows these six risk categories and some potential risk areas for future missions. The risk areas that can be mitigated directly by INTEGRITY are shown in italics.

Table 2. Risk categories and potential risk areas.

Safety	Cost	Schedule	Performance	Operations	Program
·*Equipment malfunction* ·*Accident* ·Environment	·*Estimates* ·Reserves ·Contractor performance ·*Unplanned tasks*	·*Estimates* ·Slack ·Contractor performance ·*Unplanned tasks*	·*Requirements* ·*Interfaces* ·Environment ·*Operational needs* ·*Unproven technology* ·*Software* ·*Complexity* ·*Reliability* ·*Testing*	·*Human interface* ·*Sensitivity to errors* ·*Operability* ·*Maintain-ability* ·*Testability* ·*Reparability* ·*Spares* ·*Training* ·*Communica-tions/data handling* ·*Science*	·Funds availability ·Personnel ·Facilities ·Contractor stability ·Multi-center ·Multi-agency ·International ·Environment impact ·Security ·*Political*

Risks to **safety** can be caused by a design malfunction or operations accident. These risks can be reduced by integrating, testing, and operating equipment in INTEGRITY. Obviously some equipment such as life support can be tested in INTEGRITY, and some such as orbital thrusters can not. The risks to safety from the environment include chance events such as micro-meteor impacts and solar flares and surprise hazards such as unanticipated Mars surface chemistry. These risks can not be mitigated using INTEGRITY.

Risks to **cost** are similar to risks to **schedule**. Exceeding either cost or schedule may be due to low estimates, inadequate reserve, poor contractor performance, or unexpected problems, changes, or new tasks. Producing and testing prototype equipment in INTEGRITY should improve cost and schedule estimates for flight equipment and reduce surprises due to unplanned tasks.

Risks to **performance** include incorrect requirements and interface specifications and unanticipated environmental threats or operational needs. They also involve the difficulties of unproven technology, software, complexity, and reliability. Incomplete testing can fail to uncover performance problems.

Risks during **operations** are numerous, complex, and interrelated. These include hardware and software operations, human interface, crew performance, and the "ilities." INTEGRITY is highly appropriate for mitigating operations risks by conducting operational tests and demonstrations.

Program risks are largely external to the mission, except that satisfactory progress and good performance will increase political support for human space missions beyond LEO. The progress demonstrated and the public interest generated by INTEGRITY will help increase political support.

A PRA computes the probabilities of specific undesired end states. The end states defined in the International Space Station (ISS) PRA include loss of station and crew, loss of crew, evacuation, loss of a module, loss of a system, loss of a function, and collision. [6] [7] The ISS risk analysis also includes the consequences of cost increase, schedule delay, safety reduction, and performance degradation. [8]

The undesired end states corresponding to the risk categories in table 2 are shown in table 3. The undesired end states are possible negative results of the identified risks.

Table 3. Risk categories and undesired end states.

Safety	Cost	Schedule	Performance	Operations	Program
·Loss of crew ·Crew injury ·Other injury or death ·Crew health impairment	·Cost overrun	·Schedule delay	·Performance goals not met	·Loss of base or spacecraft ·Loss of mission ·Loss of function ·Loss of science	·Project delay ·Project descoping ·Project cancellation

Design malfunction, operations accident, or environmental events can cause injury or death. Low estimates, inadequate padding, poor contract performance, or unexpected changes can cause cost overruns and schedule delays. Performance is unsatisfactory when any goal is not met for any reason. Some specific problems that may occur during missions operations are loss of a planetary base, a spacecraft, the mission, some system function, or some science product. Program problems may result in project delay, descoping, or even cancellation.

Risk, like the mission goals, is multidimensional. Safety, cost, time, and performance goals are very different things, measured on different scales. But they are exchanged for each other in the design process. The mission spends money and time to gain safety and performance. It can use cash to accelerate schedule or accept a delay to try to save money. The management task is to optimize the project parameters of safety, cost, schedule, and performance. [9] The risk analysis for INTEGRITY improves this process by explicitly identifying risks and risk mitigation.

The crewed mission PRA for INTEGRITY will estimate the probabilities and impacts of the undesired end states in table 3 for a crewed mission. This will allow the INTEGRITY program to be designed and implemented to cost-effectively reduce the most serious risks that fall within its scope.

Other useful ways to categorize risks are by project and mission phases. [10] [3] Table 4 below shows the phases of a program to conduct a generic human mission beyond LEO, similar to a moon base or Mars exploration mission. [11][10] Critical items with risks that can be mitigated directly by INTEGRITY are shown in italics.

The PRA of a human mission beyond LEO will be based on the sequential mission phases shown in table 4. Problems in the early phases of definition and design, such as a budget estimate or design error, will increase the probability of an undesired outcome in the later phases, such as a cost over run in development or a malfunction during operations. Table 3 lists the undesired end states according to risk categories, while table 4 describes the mission activities and elements that may result in these undesired end states. The mission must be decomposed as in table 4 to construct the mission PRA.

Table 4. Phases of a human mission beyond LEO.

MISSION PHASE	CRITICAL ITEMS	MAJOR RISKS
A. Preliminary analysis		
Define objectives	Mission scope	Scope too large, too small, vague
Trade alternatives	*Feasible alternatives*	Alternatives few or inadequate
Mission Definition Review (MDR)	Mission concept, *systems architecture*	Poor concept, poor architecture
B. Definition		
Preliminary Design Review (PDR)	*Budget, schedule, requirements, design concept, risk analysis*	Bad estimates, poor requirements, incomplete concept or analysis
C. Design		
Detailed definition	Meeting all requirements	Design errors
Critical Design Review (CDR)	*Budget, schedule,* design details, *risk mitigation*	Bad estimates, poor design, unresolved risks
D. Development		
Construction	Materials, procedures, quality assurance (QA)	Poor materials, procedures or QA not enforced
Integration and test	*Completeness, fidelity*	Partly untested performance
Operational Readiness Review (ORR)	*Hardware meeting all requirements safely, reliably*	Deficient system hardware
E. Operations		
Launch to Earth orbit	Booster, flight control	Booster malfunction
Planetary injection	Propulsion, flight control, navigation	Propulsion loss, heat shield failure
Planetary transit	Structure, *thermal, power, life support*	Loss of power or life support
Planetary orbit, descent, and landing	Propulsion, flight control (parachute, heat shield for Mars)	Propulsion loss
Planetary operations	Structure, *thermal, power, life support,* EVA suits, airlocks, *rover, science*	Structure leak, loss of power or life support, suit leak, accidents, rover breakdown, science equipment failure
Ascent and transit vehicle rendezvous	Booster, flight control, navigation	Booster malfunction
Return injection	Propulsion, flight control, navigation	Propulsion loss
Return transit	Structure, *thermal, power, life support*	Loss of power or life support
Earth orbit , descent and landing	Propulsion, control, parachute, heat shield	Propulsion loss, parachute or heat shield failure

PRA ILLUSTRATION

The next step is to build a high-level PRA model based on the project phases and risks identified in Table 4. However, due to the preliminary stage of this work and the extreme sensitivity to the risks to human life, we detail an unmanned planetary lander mission to illustrate a PRA. The approach, however, would be the same with the exception that there are many more undesirable states to consider besides loss of mission. Additional states could include, for example, crew injury, crew health impairment, loss of crew, and loss of base. An event sequence diagram for the illustration is shown in Figure 2 and was developed in the Netica™ software package. [12]

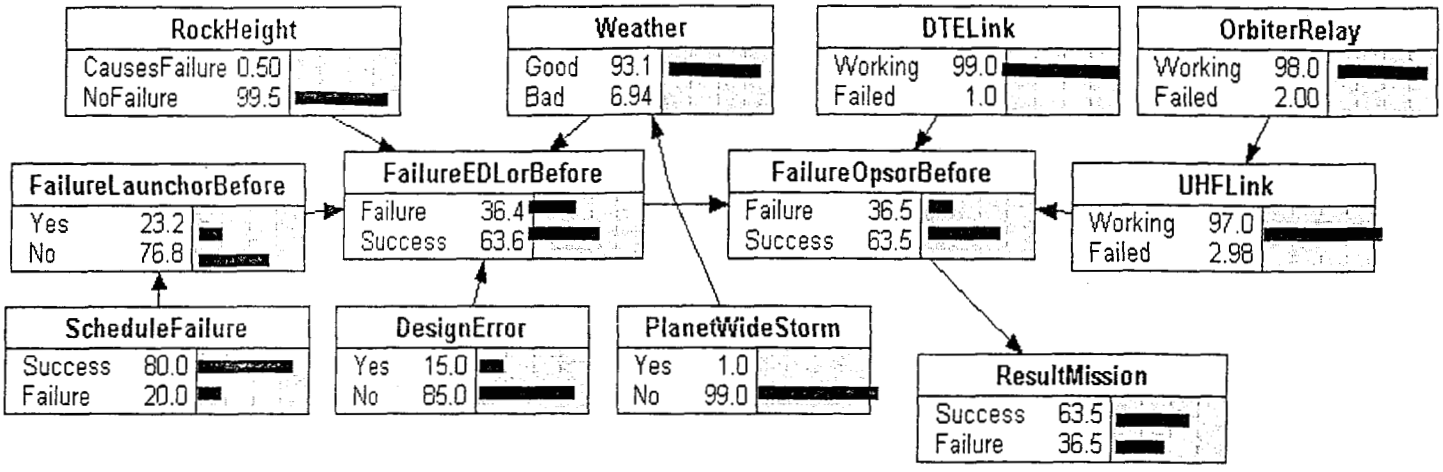

Figure 2. An event sequence diagram for an unmanned planetary lander mission.

The event sequence diagram is a compact representation of a decision tree. It is not a simple "flow chart" but a directed graph in which each node represents a random event or variable, each arrow represents a probabilistic dependence, and the final node is the result of the resolution of this diagram (and of the corresponding event tree). The diagram starts at the initiating event and progresses through a series of events until the various end states are reached – in this case the mission is either a success or a failure. Several key mission phases are identified: Pre-launch (Schedule Failure), Launch, Entry/Descent/Landing (EDL) and Operations (Ops). Each phase needs to be completed successfully or the mission fails. Each node has been defined by the name of the variable, its possible realizations, and their probabilities conditional on the realizations of the variables or events that influence it. The software then computes the final success and failure probabilities using an inference engine.

Key uncertainties that contribute to the outcome of the various stages in this example model are the rock height distribution at the chosen landing site, the weather at the landing site, the direct-to-earth (DTE) communications link, the functioning of a previous orbiter for a UHF (Ultra High Frequency) communications link, possible design errors, and possible planet wide storms.

What is represented in each box is the result of the diagram resolution, i.e., the marginal probability of each realization after combining the effects of the influencing variables. The results are represented in the final node by the probability of mission success.

Risk mitigation should focus on the highest value risks. In this illustration, we could consider different alternatives for system designs, for different landing sites, for communications, or even multiple spacecraft.

CONCLUSION

A preliminary PRA for a human space mission beyond LEO will be very useful for future missions and for INTEGRITY. The PRA should be started now, pre-phase A. The identity and severity of the undesired end states can be established and the uncertainties modeled. It is well known that 70 to 90% of a missions' scope and cost is determined by the mission definition and high-level trades conducted before and during phase A. [13] [14] To make significant changes, we must modify the mission definition during phase A, before phase B preliminary design. Missions beyond LEO are still far enough in the future, that the INTEGRITY program can have significant impacts if the program is managed to focus on projects with the greatest risk reduction benefits.

How can we perform a space mission PRA during pre-phase A? An analogy between risk analysis and cost analysis is useful. In phases C and D, design and development, the costs and risks are both estimated at the detailed component level and then aggregated from the bottom-up. At the end of phase D, the design and development costs and risks have been incurred and are known precisely, and the future (phase E, operations) costs and risks can be estimated reasonably well. In phase A, the best way to estimate cost and risk is at the highest overall system level, using similarity to other systems. (In cost analysis, the degree of system similarity is quantified using parametric cost estimating relations based on mass, mission type, etc.)

In pre-phase A and phase A, cost estimates using similarity are preferred to bottom-up estimates, which are considered unreliable. The early bottom-up failure rates estimated for Apollo were so unreasonably high that quantitative risk analysis was discredited and abandoned.

We lack the failure data, the detailed mission and system definitions, and other information needed to perform a classic detailed bottom-up PRA. Nonetheless, PRA is useful and necessary in pre-phase A. The PRA can be started with the limited information available based on expert assessments and refined as the project proceeds.

In a way, risk analysis is a self-defeating process. Whenever a significant risk is identified, it is usually mitigated. The risk analysis and mitigation process is concluded satisfactorily only when the expected risk is acceptably small. This means that any unanticipated severe failures that do occur indicate an error in the PRA process. An initiating event was not identified or was assigned too low a probability. Since the severe failure modes that PRA identifies are usually mitigated, the severe failures that do occur are often not those predicted by PRA. Despite this, doing a PRA is an excellent way to guide risk mitigation and to improve on a "gut-feel" management approach.

Because we have not yet analyzed the risks for human missions beyond LEO, it is not certain where and by how much INTEGRITY can reduce risk. But some points are obvious. Cost overruns can be expected to be roughly proportional to estimated costs. INTEGRITY is most suited to test and demonstrate the habitat, life support, crew, and human interface. Because these areas account for a significant fraction of the mission cost, INTEGRITY can help reduce cost overruns. INTEGRITY is not suitable to mitigate risks from launch malfunctions, reentry problems, EVA accidents, micrometeor impacts, etc. The operations of INTEGRITY, by reducing risk, demonstrating progress, and generating favorable attention, will reduce the risk of project cancellation and project descoping. INTEGRITY can also reduce risks for the equipment and functions it can test and demonstrate.

REFERENCES

1. Paté-Cornell, M. Elisabeth and Dean Murphy, "Human and management factors in probabilistic risk analysis: the SAM approach and observations from recent applications," *Reliability Engineering and System Safety*, vol. 53, pp. 115-126, 1996.
2. Kaplan, Stanley and B. John Garrick, "On the Quantitative Definition of Risk," *Risk Analysis*, vol. 1, no. 1, pp. 11-27, 1981.
3. D-15951, "Risk Management Handbook for JPL Projects," Appendix C, Dr. James Rose, Oct. 15, 1998.
4. Mars Global Surveyor, RISK MANAGEMENT PLAN (RMP), JPL D-12089, September 30, 1994.
5. Shishko, R., "NASA Systems Engineering Handbook," SP-6105, June 1995, NASA JPL.
6. Stamatelatos, M., "Probabilistic Risk Assessment for Program & Project Managers," p. 46, Risk Management Colloquium III, Palo Alto, California, September 17-19, 2002.
7. Smith, C., "International Space Station Probabilistic Risk Assessment," NASA PRA Practices and Needs for the New Millennium, October 25-26, 2000.
8. Perera, J. Sebastian, "International Space Station Risk Management," Risk Management Colloquium III, Palo Alto, California, September 17-19, 2002.
9. Robin L. Dillon, M. Elisabeth Paté-Cornell, and Seth D. Guikema, "Programmatic Risk Analysis for Critical Engineering Systems Under Tight Resource Constraints," *Operations Research*, May/June 2003.
10. Heydorn, R.P., and J.W. Railsback, "Safety of Crewed Spaceflight,' in Larson, W. J., and L. K. Pranke, eds., *Human Spaceflight: Mission Analysis and Design*, McGraw-Hill, New York, 2000 but undated.
11. Larson, W. J., R.B. Giffen, and R. Arno, "An Introduction to Spaceflight," in Larson, W. J., and L. K. Pranke, eds., *Human Spaceflight: Mission Analysis and Design*, McGraw-Hill, New York, 2000 but undated.
12. Netica, www.norsys.com
13. Wertz, J. R., and W. J. Larson, eds., *Reducing Space Mission Cost*, Space Technology Series, Kluwer, Dordrecht, 1996.
14. National Academy Press, *Reducing the Costs of Space Science Research Missions,* http://www.nationalacademies.org/ssb/jctmenu.html Washington, 1997.

CONTACT

Harry Jones, Ph.D.
Mail Stop 239-8
NASA Ames Research Center
Moffett Field, CA 94035-1000
Phone: 650-604-5518
e-mail: Harry.W.Jones@nasa.gov

ACRONYMS

CCF: Common-Cause Failure

CRM: Continuous Risk Management

DTE: Direct-To-Earth

EDL: Entry/Descent/Landing

ESD : Event Sequence Diagrams

ETA: Event Tree Analysis

FMEA: Failure Modes and Effects Analysis

FTA: Fault Tree Analysis

HRA: Human Reliability Analysis

INTEGRITY: INTEGRated Human Exploration Mission Simulation FacilITY

ISS: International Space Station

LEO: Low Earth Orbit

MLD: Master Logic Diagram

NPG: NASA Procedures and Guidelines

Ops: Operations

PRA: Probabilistic Risk Assessment

RBD : Reliability Block Diagrams

UHF: Ultra High Frequency