NASA's Risk Management System

Jeevan S. Perera, PhD, JD
National Aeronautics and Space Administration
Lyndon B. Johnson Space Center
Houston, Texas 77058

The views/content expressed in this presentation are solely the Author and do not necessarily represent NASA's positions, strategies or opinions

Ziff Brothers Investments Speaker Forum
November 18th, 2013
Melbourne, Australia
Agenda

- NASA’s Current Environment
- Space Exploration Systems
  - Short Video
- NASA’s Risk Management Paradigm
- Culture and Risk Management
- Risk Management Lesson Learnt
- Summary
- Q&A
NASA’s Current Uncertain Environment

President Bush’s Proposal in 2004
- Design, develop and fly the Shuttle replacement vehicle (Orion: MPCV) by 2015
- Return to the Moon around 2020
- Extend human presence across the solar system and beyond (starting with Mars)

President Obama’s Proposal in 2010:
- Collaboration with commercial sector to develop and operate “taxi services” to low-earth orbit (Shuttle replacement) – SpaceX (Falcon 9), Orbital (Taurus II) and others, etc
- Developing technologies vs. developing systems (NACA)
  - Fund technology aimed at enabling future deep-space exploration systems including new types of rocket engines /propulsion, heavy-lift launch vehicles, fueling spacecraft in orbit (on-orbit fuelling stations), etc
  - Enhance robotic exploration of space (including precursors to human missions)
  - Research and development of remote autonomous space factories for in-situ utilization
- Develop a simplified MPCV vehicle to provide multipurpose utility for space explorations. Also, use MPCV as part of the technological foundation for advanced spacecraft for future deep space missions.
- Human exploration to asteroids (2025) and eventually Mars (2030s)
- Foster more International collaboration on future missions/projects (e.g. ISS)
- Initiate development of a heavy-lift launch vehicle and ready by 2017
Launch Vehicle Comparisons

**Space Shuttle**
- Height: 184.2 ft
- Gross Liftoff Mass: 4.5M lb
- 55k lbm to LEO

**Ares I**
- Height: 321 ft
- Gross Liftoff Mass: 2.0M lb
- 48k lbm to LEO

**Saturn V**
- Height: 364 ft
- Gross Liftoff Mass: 6.5M lb
- 99k lbm to TLI
- 262k lbm to LEO

**Falcon 9**
- Height: 180 ft
- Gross Liftoff Mass: 0.7M lb
- 23k lbm to LEO
- 10k lbm to GTO

**Dragon**
- Volume: 245 ft³ (pressurized)
- Payload Up Mass: 13k lbm
- Up to 7 crewmembers

---

Upper Stage
(1 J-2X)
280k lb LOx/LH₂

5-Segment
Reusable Solid Rocket Booster (RSRB)

5-Segment
(1 J-2 engine)
240k lb LOx/LH₂

S-II
(5 J-2 engines)
1M lb LOx/LH₂

S-IC
(5 F-1)
3.9M lb LOx/RP

Crew
Lander

2nd Stage
(1 SpaceX Merlin)
LOx & RP-1

1st Stage
(9 SpaceX Merlin)
Vocabulary

- Extensive list of terms and definitions to establish a common vernacular for effective communication and management of risk

- Examples:
  - *Risk* – A measure of the potential inability to achieve a goal or target within defined safety, cost, schedule, and technical constraints. It has two components: (1) the likelihood (or probability) of failing to achieve a particular outcome, and (2) the consequence (or impact) of failing to achieve that outcome.
  - *Risk Management* – a process for identifying and mitigating threats to achieve safety, cost, schedule, and performance requirements. It assists in making decisions on budget and resource allocation to meet objectives.
  - *Risk Owner* – The individual to whom the risk is assigned for purposes of responsibility, authority, accountability and given resources to address an assigned risk. Manages, coordinates, and tracks the risk mitigation approach and actions.
NASA Risk Management Principles

♦ Creates Value
  ▪ Use risk-informed decision to prioritize strategic and operational decisions
  ▪ Apply practices to ensure planned objectives & missions are fully achieved
  ▪ Synthesize projects and allocate risk and organization resources optimally
    - Manage risks by developing comprehensive risk handling to minimize life cycle costs

♦ Integrated in Organizational Processes
  ▪ A formally documented risk management process
    - Extensive and Tiered Training
  ▪ Integrate risk management into overall project management with comprehensive, structured and integrated processes
  ▪ Manage risks at the lowest level possible (where the subject matter experts)
NASA Risk Management Principles

♦ Part of Decision Making
  ▪ Improve the quality of decision-making throughout the organization
    - Even seemingly insignificant risks on their own have the potential, as they interact with other events and conditions to cause great damage.
  ▪ Risk is a part of every decision made
  ▪ *ISS Vozdukh vs. SM Window Cover Example*

♦ Explicitly Addresses Uncertainty
  ▪ The uncertainties related to the knowledge and context of the risk
  ▪ The uncertainties that the risk creates on objectives/goals

♦ Systematic, Structured and Timely
  ▪ Require risk identification and management to occur in a tiered, integrated, structured manner
  ▪ Routine risk management at all tiers of the organization
  ▪ Comprehensive and structured risks identification processes and tools
  ▪ Proper incentives and disincentives to foster good practices
NASA Risk Management Principles

- Based on the Best Available Information
  - Risk Owners are subject matter experts on the “front lines”
  - Risk register (database) updated with current information by risk owner
  - Analyze how individual risks aggregate or are interrelated. Analyze for systemic problems and overall trends.

- Takes Human and Cultural Factors into Account
  - Processes fit culture and organizational structure of NASA
  - Reinforce the values of radical transparency and continuous improvement.
NASA Risk Management Principles

- **Transparent and Inclusive**
  - All team members are responsible for risk management
    - Clearly defined Roles and Responsibilities
  - Risk meeting/committee are open and free.
  - Risk database is open (concerns closed)
  - Accountability - assign risk ownership
  - Dissenting opinions are encouraged
    - Examples

- **Dynamic, Iterative and Responsive to Change**
  - Information is flowed up, resources and prioritizations are flowed down, while coordination is made with all responsible stakeholders
  - Facilitates Continual Improvements and Enhancement of the Organization
    - Remove roadblocks preventing entry into risk management
    - Ongoing monitoring activities are conducted to continually assess risks and risk plans
    - Monitoring and review of risk management effectiveness (metrics)
    - Audit and surveillance (internal and external)
Framework

Mandate & Commitment
- Allocation of Resources
- Setting Goals and Expectations
- Defining Risk Appetite

Design of the Framework
- Phased Approach
- Defining requirements based on Principles and needs
- Adjustments to increase effectiveness

Continual Improvement of the Framework
- Internal Assessments of Framework
- External surveys of best practices

Implement the Framework
- Ensure implementation

Monitor, Review and Assess Framework
- Metrics
- Surveys
Sources of Risk

- External Events
  - Hurricanes
  - Earthquakes
  - Floods
  - Fire

- Human Errors
  - Inattention
  - Error
  - Misdiagnosis
  - Sabotage

- Institutional Failure
  - Training
  - Poor Communications
  - Unclear Roles/Responsibilities
  - Morale
  - Management Attitude

- Equipment Failure
  - Independent Failures
  - Common Cause Failures
RM Tools & Techniques

**QUANTITATIVE**
- Stochastic and Deterministic Modeling
  - Probabilistic Risk Assessments (PRA)
  - Other Statistical based Modeling and Analysis techniques
- Cause & Effects Analysis
  - Failure Modes & Effects Analysis (FMEA)
  - Fault Tree Analysis (FTA)
- Systems Engineering Analysis and Risk Assessments
- Cost and Schedule Analysis

**QUALITATIVE**
- Root Cause Analysis
- Hazard Analysis
- Brainstorming
- Process Mapping and Analysis (Human Factors)
- Taxonomy-Based Questionnaires
- Pareto Method
- Affinity Grouping
Risk Coordination and Integration

* Internal and external stakeholders are included at the appropriate tier level
## ORION (CEV) RISK SCORECARD

### Likelihood Rating

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Very High</td>
</tr>
<tr>
<td>4</td>
<td>High</td>
</tr>
<tr>
<td>3</td>
<td>Moderate</td>
</tr>
<tr>
<td>2</td>
<td>Low</td>
</tr>
<tr>
<td>1</td>
<td>Very Low</td>
</tr>
</tbody>
</table>

### Consequence Rating

<table>
<thead>
<tr>
<th>Consequence Rating</th>
<th>1 - Very Low</th>
<th>2 - Low</th>
<th>3 - Moderate</th>
<th>4 - High</th>
<th>5 - Very High</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Safety</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personnel</td>
<td>A condition that could cause the need for minor first aid treatment though would not adversely affect personal safety or health (Class IV)</td>
<td>A condition that may cause minor injury or occupational illness (Class III)</td>
<td>A condition that may cause severe injury or occupational illness (Class II)</td>
<td>A condition that may cause permanently disabling injury (Class I-B)</td>
<td>A condition that may cause death or loss of crew (Class I-A)</td>
</tr>
<tr>
<td>Facilities, Equipment, or Other Assets</td>
<td>A condition that subjects facilities, equipment, or flight hardware to more than normal wear and tear (Class IV)</td>
<td>A condition that may cause minor property damage to facilities, systems, equipment, or flight hardware (Class III)</td>
<td>A condition that may cause major property damage to facilities, systems, equipment, or flight hardware (Class II)</td>
<td>A condition that may cause destruction of non critical facilities or assets (Class I-B)</td>
<td>A condition that may cause destruction of critical facilities on the ground, major systems, or vehicle during the mission (Class I-A)</td>
</tr>
<tr>
<td>Environment</td>
<td>Negligible OSHA/EPA violation - non reportable</td>
<td>Minor reportable OSHA/EPA violation which requires immediate remediation</td>
<td>Moderate OSHA/EPA violation causing temporary stoppage</td>
<td>Major OSHA/EPA violation resulting in action terminating project</td>
<td>Serious or repeat OSHA/EPA violations resulting in action terminating project</td>
</tr>
<tr>
<td><strong>Performance</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Including impacts to operations and supportability</td>
<td>Negligible impact to requirements, mission objectives or technical goals</td>
<td>Minor Impact to requirements, mission objectives or technical goals</td>
<td>Moderate impact to requirements, mission objectives or technical goals</td>
<td>Major impact to requirements, mission objectives or technical goals</td>
<td>Technical goals not achievable with existing engineering capabilities/technologies</td>
</tr>
<tr>
<td><strong>Cost</strong></td>
<td>$&lt;100k (Negligible impact to budget)</td>
<td>$100k but $&lt;1M (Moderate impact to budget)</td>
<td>$1M but $&lt;10M (Major impact to budget)</td>
<td>$10M but $&lt;50M (Possible project cancellation)</td>
<td>$&gt;50M (Possible project cancellation)</td>
</tr>
<tr>
<td><strong>Schedule</strong></td>
<td>Negligible schedule impact</td>
<td>Minor overall schedule impact (Accommodate with reserve, no impact to critical path)</td>
<td>1 month impact to critical path/milestones</td>
<td>1 month impact to critical path/milestones</td>
<td>5 month impact to critical path/milestones or possible project cancellation</td>
</tr>
</tbody>
</table>

### Risk Matrix

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Class I</td>
</tr>
<tr>
<td>4</td>
<td>Class II</td>
</tr>
<tr>
<td>3</td>
<td>Class III</td>
</tr>
<tr>
<td>2</td>
<td>Class IV</td>
</tr>
<tr>
<td>1</td>
<td>Class V</td>
</tr>
</tbody>
</table>

### Timeframe

- **Near**: 0 to 3 months
- **Mid**: 3 to 9 months
- **Far**: > 9 months

### Handling Strategy

- **Time to Initiate**:
  - Near: 0 to 3 months
  - Mid: 3 to 9 months
  - Far: > 9 months

**September 2006**
Organizational Culture & Risk Management

- Organization’s culture not only consists of interlocking set of goals, roles, processes, values, communications practices, attitudes and assumptions, but also many nebulous and dynamic elements
  - Changing organizational culture is one of the most difficult things to change

- Fundamental elements in changing organizational culture
  - **Where are you now:** understand the current culture.
  - **Where do you want to be:** decide where it wants to go, define its strategic direction, and decide what the organizational culture should look like to support success. What vision does the organization have for its future and how must the culture change to support the accomplishment of that vision?
  - **Is there a road there:** the organization’s people must decide to change their behavior to create the desired organizational culture.
    - Cognitive – people must have some understanding of why the change in strategy or in culture is needed.
    - Motivation – ultimately, workers have to want to make the change (incentives/disincentives).
Culture

- **Reporting Culture:** We report our concerns. Identification of hazards or safety concerns is encouraged, including a system that’s easy to use. The reporting system maintains anonymity and is separate from the disciplinary processes. Useful feedback based on reporting is quick and insightful. An atmosphere of trust exists between managers and workers, with employees knowing important information will be voiced, heard, and acted on appropriately.

- **Just Culture:** We have a sense of fairness. People are held accountable for deliberate violations of rules and recognized for outstanding performance. There’s a clear understanding of acceptable and unacceptable behaviors. There’s a sense of fairness about how business is conducted, where people aren’t punished for reporting and aren’t afraid of reprisal if they do.

- **Flexible Culture:** We change to meet new demands. The organization effectively balances and adapts to changing demands. A healthy flexible culture uses safety data to make meaningful changes when there’s a concerning trend or issue.

- **Learning Culture:** We learn from our successes and mistakes. Collecting, assessing, and sharing from experience is a priority. Information is available to everyone from novice to expert. Values and commits to proactively "learn from our mistakes," both formally and informally.

- **Engaged Culture:** Everyone does their part. All members regardless of status or occupation are involved and actively participate in safely accomplishing the mission. The key is to have leaders and employees who demonstrate they value safety by "walking the talk."
Risk Management Lessons Learnt

- Risk management supported by leadership, team members and stakeholders and active involvement by all
  - Uses it and promotes it

- A well defined, structured and understood risk management processes and tools
  - All team-members are expected to participate in risk management
  - A formally documented risk management process
  - A proactive risk training program
    - Not overly complex, must be understood and used (minimize overhead & foster adherence)
  - Comprehensive and structured risks identification processes and tools
    (Establish risk toolbox for identifying and analyzing risks)
  - Proper incentives and disincentives to foster good practices
  - Phased implementation approach

- Continuous and iterative assessment of risks
  - Provide elements of independence of the risk analysis function from the program/project
Risk Management Lessons Learnt

- Integrated with program/project decision-making processes (RIDM)
  - Continuous, event-driven technical reviews (incl project milestones) to help define a program that satisfies the customer’s needs within acceptable risk
  - Continuous prioritization, assessments and mitigation planning and appropriate funding

- Risk management integral to the acquisition process
- A continuous process improvement strategy that monitors and improves risk management processes and tools
- Weaving Risk Management into the cultural fabric of the organization is critical, but difficult
Summary

- Phased-approach for implementation of risk management is necessary
- Risk management system will be simple, accessible and promote communication of information to all relevant stakeholders for optimal resource allocation and risk mitigation
  - Risk management should be used by all team members to manage risks – not just risk office personnel
  - Each group/department is assigned Risk Integrators who are facilitators for effective risk management
  - Risks will be managed at the lowest-level feasible, elevate only those risks that require coordination or management from above
- Risk informed decision making should be introduced to all levels of management
- Provide necessary checks and balances to insure that risks are caught/identified and dealt with in a timely manner
- Many supporting tools, processes & training must be deployed for effective risk management implementation
- Process improvement must be included in the risk processes
Questions?