A Look Back At The Risk Management Of The Space Shuttle Programme & A Look Forward To NASA's Risk Management Strategy For The Future

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

Ri$kMinds 2011
Geneva, Switzerland
7 December, 2011

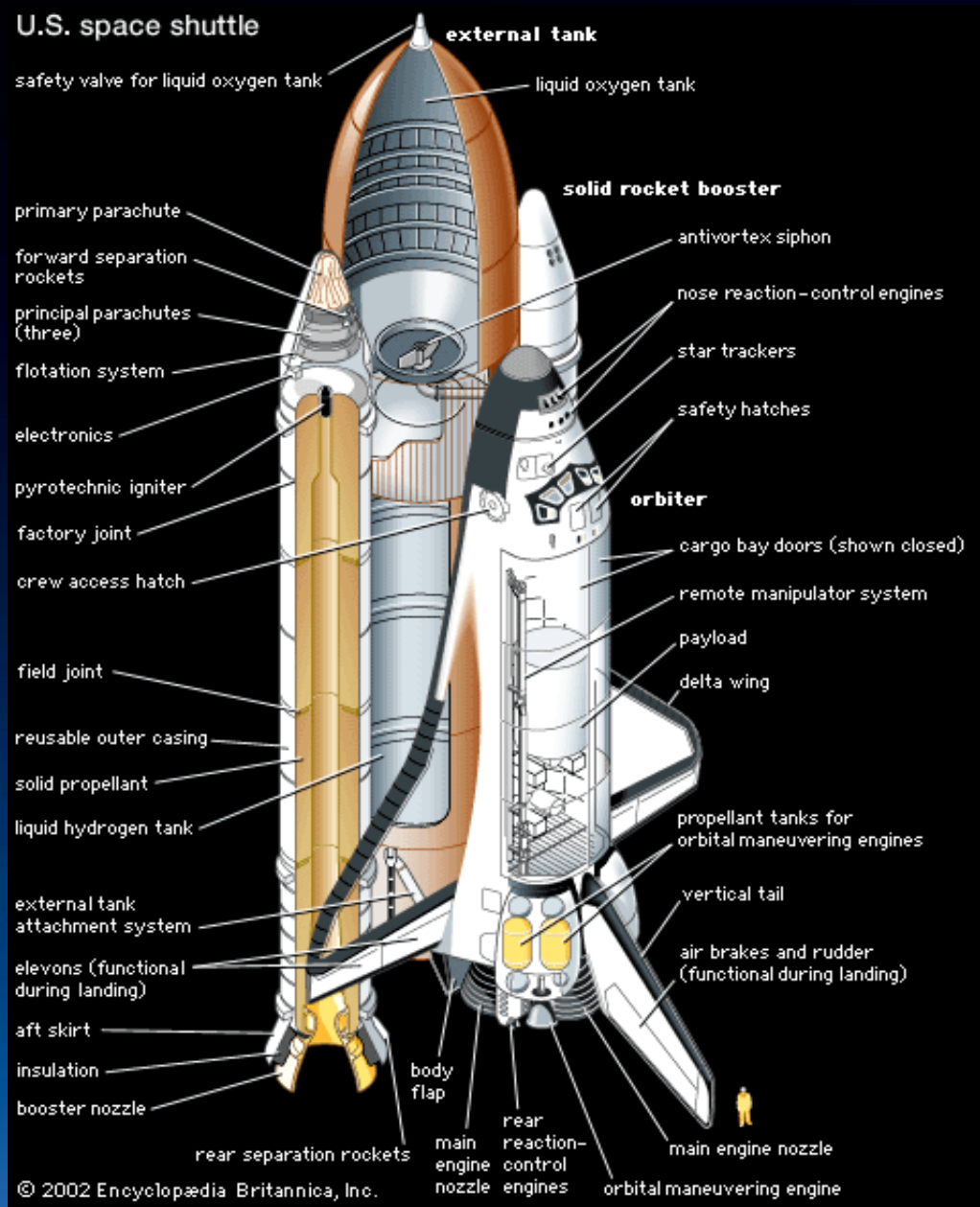
The views/content expressed in this presentation are solely the Author and do not necessarily represent NASA's positions, strategies or opinions

Agenda

- NASA's Current Environment
- A Retrospect of the Space Shuttle
- NASA's Risk Management Paradigm
- Risk Management Lesson Learnt
- Summary
- Q&A

Space Shuttle Overview

- Orbiter Vehicle
- Solid Rocket Boosters (SRB)
- External Tank (ET)

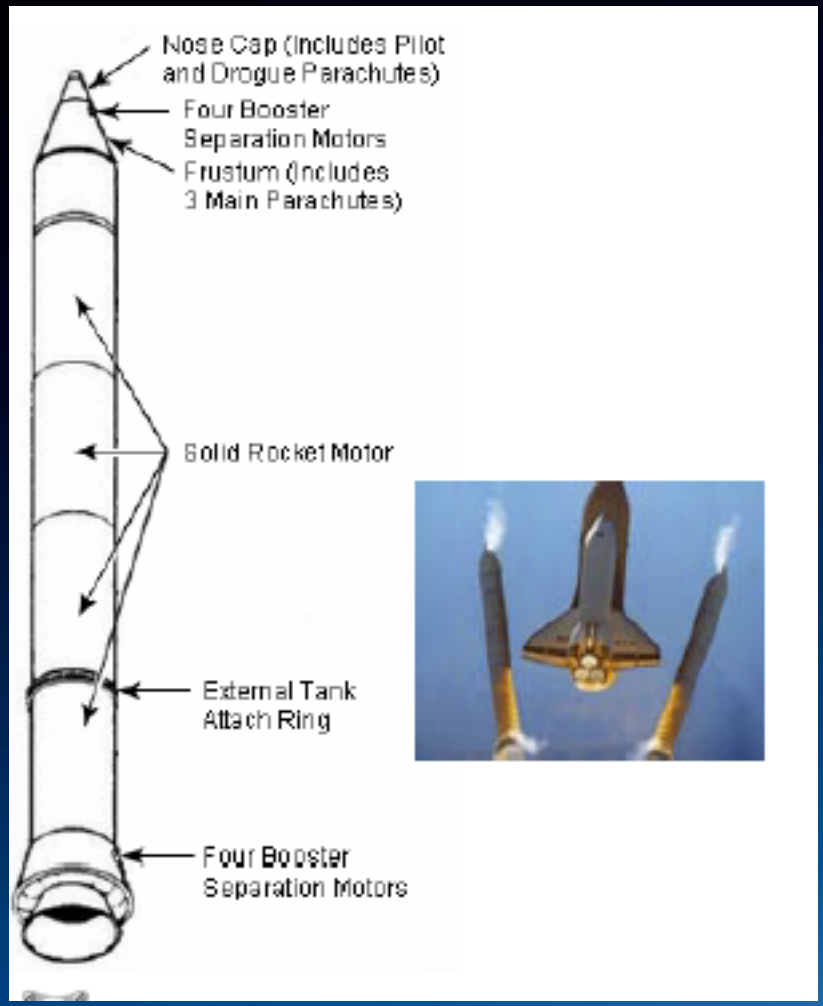


Space Shuttle Main Engines (SSME)

- 3 located on aft of Orbiter (weighs 7000 lbs each)
- Burns liquid oxygen and liquid hydrogen
- Each engine generates 400,000 lbs of thrust (all SSMEs provide 29% thrust at liftoff)
- Burn for 8.5 minutes after liftoff

Solid Rocket Boosters (SRB)

- Largest solid rocket motors and first designed to be reusable
- Each weighs 1.3M lbs and produces 3.3M lbs of thrust (both produce 71% of thrust at liftoff)
- Burns for 2 minutes after liftoff



Other Major Systems

- Orbital Maneuvering System (OMS)
  - 10.5 minutes after liftoff to put Orbiter in orbit
  - Used to slow Shuttle down for de-orbit
- Reaction Control System (RCS)
  - Maneuvering engines to control Shuttle in Space (i.e., docking maneuvers)
- External Tank (ET)
- Flight Deck & Mid Deck
- Airlock
- Payload Bay and SSRMS
- ECLSS
  - Pressure Control System
  - Atmospheric Revitalization System
  - Active Thermal Control System
  - Supply and Wastewater System

Shuttle Video

Risk Management Paradigm

Sources of Risk

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) & Failure Modes, Effects & Criticality Analysis (FMECA)
  - Fault Tree Analysis (FTA)
- Systems Engineering Analysis and Risk Assessments

QUALITITATIVE

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

Enterprise Risk Management

- Primary purpose of ERM is to improve the quality of decision-making throughout the organization
  - **Help prioritize strategic and operational decisions**
  - **Ensure planned objectives & missions are fully achieved**
  - **Synthesize projects and allocate risk and agency resources optimally**
  - **Improve mission & project performance to meet agency goals**
    - Projects delivered on time, on budget within requirements/specifications
- Treating risks in a holistic manner
  - **Managing all risks and their interactions effectively (not just within silos). Done at the agency level not just at the traditional project or program level**
    - Consistency of risk processes and the mitigation of risks
    - Even seemingly insignificant risks on their own have the potential, as they interact with other events and conditions to cause great damage.
  - **Risk management becomes part of overall project management with comprehensive, structured and integrated processes**
  - **Integrated and synthesize Risks & Opportunities, Contingency Planning, Crisis Management, Continuity of Operations, Disaster Recovery, etc.**
  - **Facilitate structured communications throughout the organization and with all stakeholders (internal & external) – avoid filtering of information**

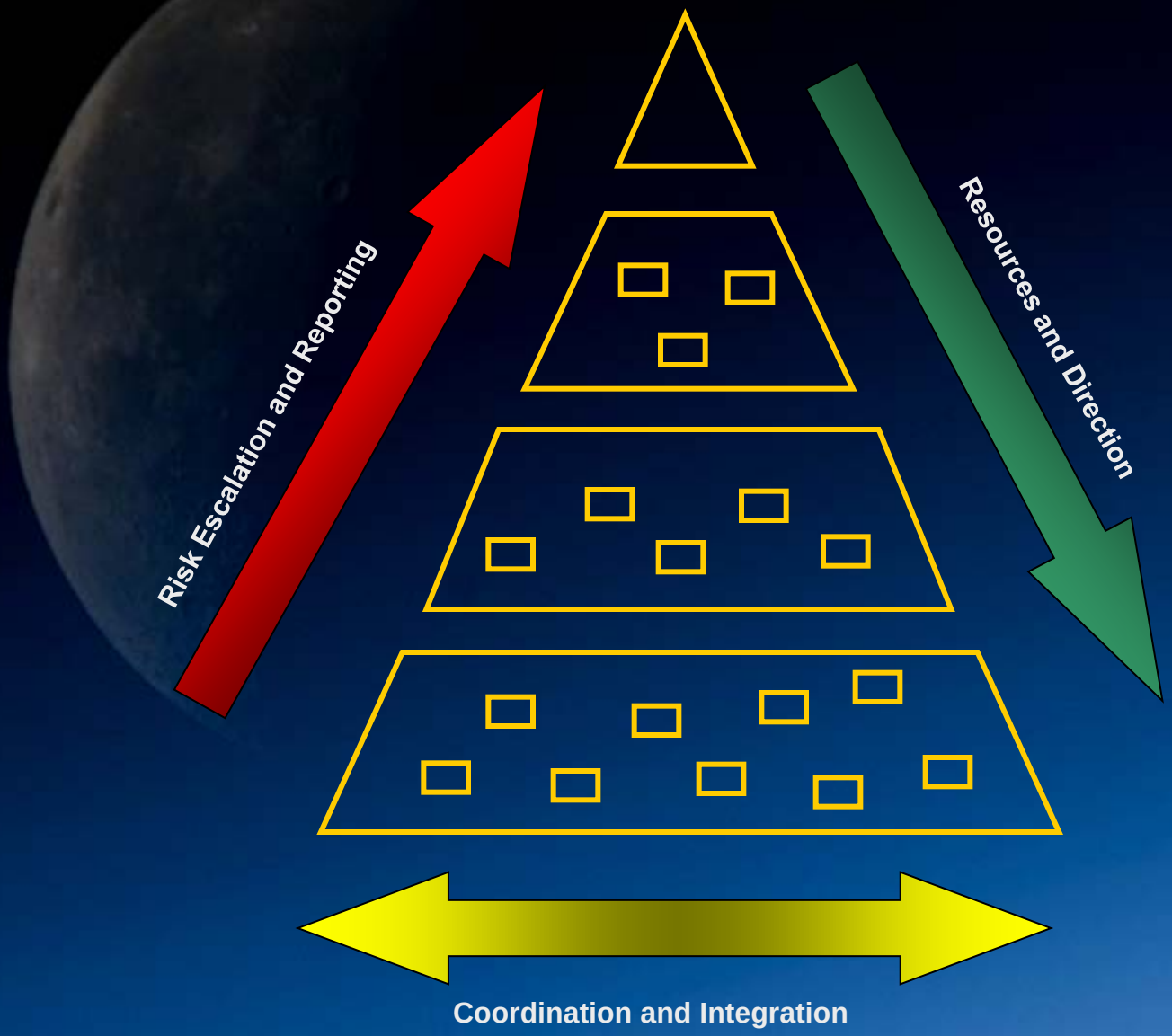
Risk Management Implementation Strategy

- Covers all phases of the life cycle
- Provide a risk management communication infrastructure to store, analyze and deal with problems proactively – overlay on existing management infrastructure
  - **Deploy the risk process, tools and systems within the whole enterprise and integrate with other management systems (integrate risk management with other programmatic functions, including safety & mission assurance, system engineering, analysis and project control/cost & schedule) and also within contractors/subcontractors and supplier base.**
- Require risk identification and management to occur in a tiered, integrated, structured manner
  - **Remove roadblocks preventing entry into risk management system (ensure risk management accessible to all levels of the organization)**
  - **Analyze and individually quantify the risk consequence categories (e.g., Safety, Performance, Schedule, & Cost) for comprehensive understanding of risk impacts – to aid in risk prioritization**
  - **Analyze how individual risks aggregate or are interrelated. Look for systemic problems and overall trends.**
  - **Manage risks by developing appropriate risk handling/mitigation strategies (assign resources based on prioritization) & then monitor/control (include all necessary stakeholder assistance to ensure comprehensive closure) – prepare fall-back plans**
  - **Accountability - assign risk ownership to the individual best suited to effectuate effective closure (usually the technical expert). Risk owner is responsible for shepherding the risk through closure and coordinating with all players.**
  - **Dissenting opinions are encouraged – they are documented and evaluated within the standard risk processes**

Risk Management Implementation Strategy

- Prioritize and escalate risks appropriately, only escalate issues that need resolution from above
  - **Prioritization includes Cost/Benefit Analysis**
  - **Information is flowed up, resources and prioritizations are flowed down, while coordination is made with all responsible stakeholders**
  - **Manage risks at the lowest level possible where the subject matter experts are and where it is the easiest to implement risk mitigation strategies and monitor its effectiveness**
  - **Ensure that risks receive the appropriate level of management review and resources to effectively mitigate significant threats as early as possible (as cheaply as possible). Risks will be presented at each management level**
- Criteria for Risk escalation (to the next level): Risks should be elevated to the next level control board for discussion if:
  - **A decision is needed by the next level management or higher**
  - **Additional resources are required to effectively mitigate the risk**
  - **Coordination/Integration is needed with other organizations/stakeholders outside the current level**
  - **Awareness or visibility by the next level management or higher is generally needed**
- Ongoing monitoring activities are conducted to periodically reassess risk and the effectiveness of controls to manage risk

Risk Coordination and Integration



- Program Manager
- Project Managers
- Element Managers
- System Managers
- Team Members
- Contractors/suppliers/ vendors

ORION (CEV) RISK SCORECARD

LIKELIHOOD RATING

5	Very High	Qualitative: Likely to occur. Quantitative: 10^{-1} <P (for risks with primary impact on human safety) or P>50% (for risks with primary impact on cost, schedule, or performance)
4	High	Qualitative: Probably will occur. Quantitative: 10^{-2} <P≤10^{-1} (for risks with primary impact on human safety) or 33%<P≤50% (for risks with primary impact on cost, schedule, or performance)
3	Moderate	Qualitative: May occur. Quantitative: 10^{-3} <P≤10^{-2} (for risks with primary impact on human safety) or 10%<P≤33% (for risks with primary impact on cost, schedule, or performance)
2	Low	Qualitative: Unlikely to occur. Quantitative: 10^{-6} <P≤10^{-3} (for risks with primary impact on human safety) or 1%<P≤10% (for risks with primary impact on cost, schedule, or performance)
1	Very Low	Qualitative: Occurence improbable. Quantitative: P≤10^{-6} (for risks with primary impact on human safety) or P≤1% (for risks with primary impact on cost, schedule, or performance)

RISK MATRIX

LIKELIHOOD	1	2	3	4	5
5	10	16	20	23	25
4	7	13	18	22	24
3	4	9	15	19	21
2	2	6	11	14	17
1	1	3	5	8	12

CONSEQUENCES

TIMEFRAME

Near	0 to 3 months
Mid	3 to 9 months
Far	> 9 months

Time to Initiate Handling Strategy

IMPACTS TO CEV GOALS

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

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
  - A formally documented risk management process
  - Comprehensive and structured risks identification processes and tools (Establish risk toolbox for identifying and analyzing risks)
  - Proper incentives and disincentives to foster good practices
  - All team-members are expected to participate in risk management
  - Not overly complex, must be understood and used (minimize overhead & foster adherence)
  - A proactive risk training program
- Continuous and iterative assessment of risks
  - Provide elements of independence of the risk analysis function from the program/project
- 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 – risk office personnel
  - Each group 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 reporting and communication is an essential element of risk management and will combine both qualitative and quantitative elements
- 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?