

SPACE SYSTEMS ENGINEERING AND RISK MANAGEMENT – JOINED AT THE
HIP

DRAFT

Dr. James R Rose
Risk Management Process Owner
Jet Propulsion Laboratory (JPL)
MS 156-252
4800 Oak Grove Dr
Pasadena California
e-mail:
james.r.rose@jpl.nasa.gov

Abstract

The development of an Aerospace System involves a disciplined technical and management oversight for which a unique methodology of space systems engineering has evolved and been instrumental in the success of space missions since nearly the dawn of the exploration and utilization of outer space. In the current era of cost-constrained, technically demanding, technology-rich missions, systems engineering is changing again to encompass the similarly disciplined but less mature methodology of space mission risk management. In this growing relationship, systems engineering is beginning to embrace the non-technical third leg of the successful space endeavor stool – accomplishing the job within the budget and on schedule – an area where space systems risk management has focused its attention from its inception.

The integrated disciplines of systems engineering and systems engineering-related processes, and the risk management process, fused with a basis of cost/ performance/ risk trade-off capabilities and decision analysis, can provide the structured basis project managers need for successfully bringing in today's space missions within cost and schedule.

This paper explores the separate skills and capabilities practiced until now, and the powerful coupling to be achieved, practically and effectively, in implementing a space mission, from inception (pre-phase A) to the end of Operations (phase E). The use of risk assessment techniques in balancing cost risk against performance risk, and the application of the systems engineering team in these trades, is the key to achieving this new implementation paradigm.

Outline:

- Introduction
- Integrating Risk in Early Project Phases
- Risk in Procurement of Project Elements
- Risk in Design and Development
- Risk in Verification, Validation, and Commitment
- Conclusions

1 Introduction

Systems engineering in the Aerospace industry is conducted in a variety of ways among the different organizations. Some organization recognize systems engineering as a distinct organizational capability independent from but parallel with the technical disciplines, while others identify it as an engineering discipline similar to guidance and control, electrical/ power, structures and mechanics, etc. However the function is organized, there are some common objectives of systems engineering applied to the successful development of a flight project. These tend to be of two generic types:

- a) Overview and coordination functions
- b) Engineering specialties such as systems electrical interface design and control, fault protection design, operations scenario development, etc.

Systems engineering in some organizations encompasses system-wide functions such as make-buy acquisition strategy, product assurance and reliability, and the other “ilities” or broad systems-view disciplines. These also can be significantly more effective when integrated with the risk management methodology.

Key functions performed by systems engineers are the development of system requirements and their flow-down to the subsystem/ design engineers, validation of the design, and verification and validation of the resultant product.

In the course of the project’s developing the design and delivering the product, systems engineers also play a key role in defining the design, and solving problems which occur during the processes of design, development and test. Finally, systems engineers are often important members of the operations teams – coordinating and checking the daily instructions for consistency and safety in accomplishing the mission objectives.

The area where systems engineering is often only peripherally involved is considering and controlling the cost and schedule of the development process. While technical performance and optimum design for reliable operations are the focus, and effective methodologies, expertise, and tools are brought to

bear in these areas, systems engineers have relatively poor understanding of how to determine the real cost and time required to implement a design, and also are not trained or equipped to effectively determine the integrated cost and schedule impact of the recovery from a problem which has occurred along the way.

Risk management on a Flight Project has the responsibility to oversee the project's successful passage through the technical and programmatic minefields that threaten mission success. Just as with systems engineering, this discipline also has the whole project view as its scope. As defined by NASA and implemented at JPL, risk management looks equally at the design implementation and operational performance of the system. Risk management assesses the risk to satisfying mission requirements **and** to launching and operating within budget and schedule. At JPL, risks are assessed for both their **mission risk** component, and their **implementation risk** component. A limitation to the effectiveness of, risk management on most projects is that its application is quite subjective, and assessments of the consequences and likelihoods of the risks are qualitative. Quantitative assessments similar to those systems engineers use to make good design decisions are the exception, not the rule.

Combining these two disciplines to provide systems engineering overview and quantitative analysis of mission and implementation aspects, bringing to bear on risk assessment the disciplines and tools of quantitative analyses and trade-off methods should improve the balance of success of flight projects in this programmatic era of competitive, cost-constrained programs. At the same time, adding the risk dimension to all programmatic planning and technical definition efforts can provide real insight into the most likely effort and cost required to be successful.

2 Integrating Risk in Early Project Phases

The JPL Project Life-Cycle is shown on Fig 1. The activities of Systems Engineering and Risk Management are illustrated. Discussions in this paper will refer to the life-cycle activities and their shifts as the project matures.

Early in the project planning process, two major activities take place. The definition of the technical product – spacecraft, payload, mission, operations approach, and provision of required data – is the major task of the systems engineers, while determining the resources and time required to implement the project is coordinated by project planners and takes place concurrently. All of this is accomplished in most cases to fit within a set of cost and schedule constraints and guidelines.

The interaction between these technical and programmatic disciplines provides understanding of the bounds of expectations, and leads to a design

concept which provides balanced return for the customers (scientists, potential users of the data) within the constraints. At JPL, this planning is beginning to look to risk as an integrating parameter in this effort. The project is assessing the risk areas, both technical/ performance, and implementability, and trying to assess them in a common framework. This hopefully allows well-justified design and programmatic decisions, including reasonable but not excessive understanding of the required reserves to be set aside. These project definitions and risk assessments are packaged in plans prepared to allow the customer to approve proceeding into the next, more costly phase of implementation.

Risks identified at this stage are not very definitive, and carry great uncertainties on the assessment of likelihood and impact, and thus the quantified risk cost. They do provide insight into a methodological assessment of the proposed effort, and some justification for reserves that might be outside the normal guidelines.

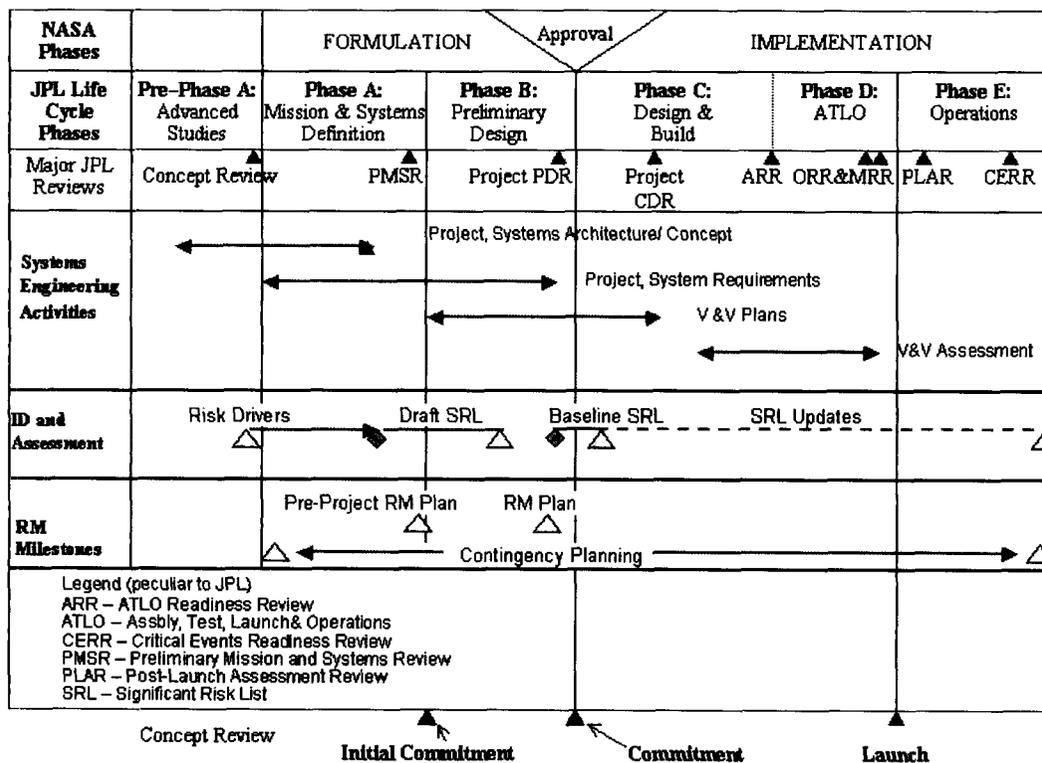


Fig 1 –Systems Engineering and Risk Management in the JPL Life Cycle

We are beginning to provide substantially greater, more comprehensive interaction between risks and project definition in these early phases. They

involve the trade-off process led by systems engineers, and involve aspects of the risk management methodologies for identifying risk.

Cost and Schedule Risk-Based Planning

To integrate risk into cost and schedule estimates, project planners at JPL in the formulation phase are in the process of developing acceptance of risk-based reserve planning. Figure 1 illustrates the objective of providing quantitative impacts in cost and schedule for each risk identified in the early planning risk list. Technical risks are costed by determining what a response might be, and to what work areas these costs might be assigned. Resource loaded network schedules provide estimates of the cost element of schedule increases.

In figuring appropriate reserves, JPL applies rules-based reserves, to handle “unknown-unknowns” (those risks which are not assessable individually, but in the aggregate have historical predictability). However, when specific risks are identified and assessed, they can with this process be integrated into the identification of reserves for risk mitigation/ exposure.

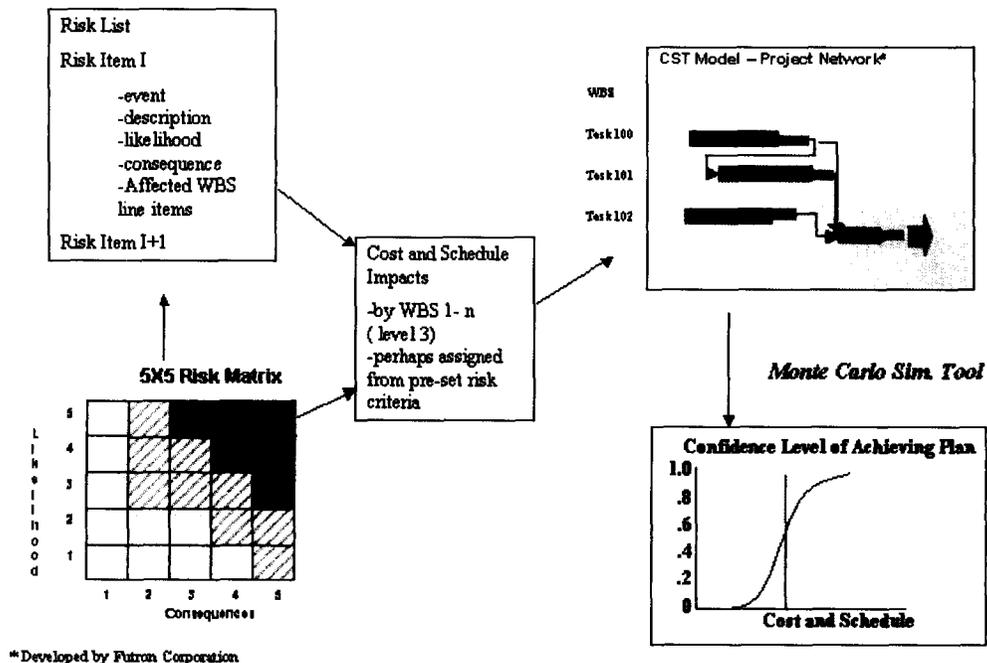


Fig 2 Incorporating Risk in Resource Estimation

This process allows the project to think through the consequences and responses to risk, and incorporate an uncertain, yet objective reserve factor. It has the additional benefit of integrating the cost impact of schedule increases along with the increased cost to recover from the risk. While achieving some success in establishing credible bases for cost estimates of proposed new projects, there is even more benefit to be realized in applying it to cost management in the project being implemented, and this is the next focus of risk-based project management.

3 Risk in Procurement of Project Elements

In the current environment of NASA Space Exploration, many projects are implemented each year of moderate size (small - \$25M to \$75M, medium – up to \$250- \$300M, and a few large – up to \$700M - \$900M), and most of these at JPL involve major partnerships with industry. Even “in-house” missions such as Mars Exploration Rover involve critical procurements of components of the flight systems, and major instruments. This has led NASA to develop a Risk Based Acquisition Management process (RBAM), where systems engineers, project managers and risk managers tie the procurement to the overall risk posture and assessment of the project.

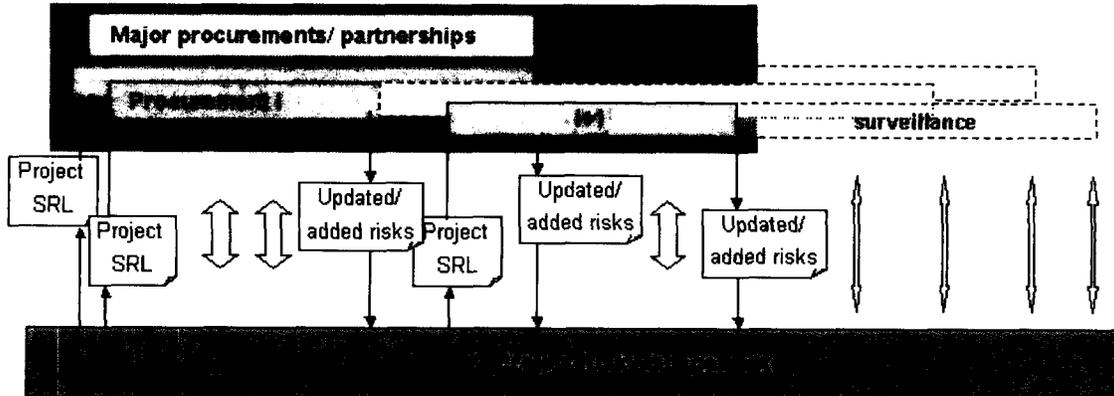


Fig 3 Risk Management in Flight Project Acquisitions

Figure 3 illustrates the major interfaces between Risk Management and the Acquisition processes. The project develops as definitive a list of risks as possible at this early stage of the implementation phase. Some of the project risks will involve the item being procured. The acquisition process uses the applicable risks to begin an acquisition-focused risk list. This list is developed in much the same way as the project’s list – with a combination of comprehensive identification and assessment methods (checklists, lessons learned, etc.) and workshop-like brainstorming sessions with the acquisition planning team.

Included are risks due to nature of the product and others are risks in the acquisition plan itself (e.g. a too- short fact-finding period could result in an inadequate “most likely cost” assessment). These risks are used to

- a) Plan the solicitation (RFP, technical requirements, deliverables, proposal content, etc.)
- b) Define the evaluation criteria and process, and
- c) Structure the surveillance plan

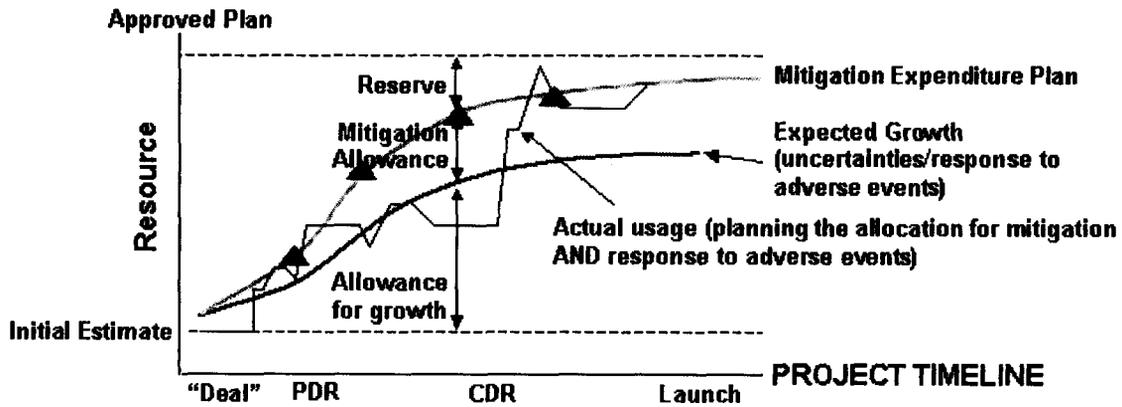
Proposers are asked to address risks identified by the project, as well as to identify and assess the risks they see, using the same assessment criteria used by the project.

Risks are adjusted, mitigated, resolved etc. as the procurement proceeds, and reported to the Project and Institute as appropriate. Finally, when the contracts are finalized, the residual and resultant risks are fed back into the project risk process. These risks are addressed in structuring the final surveillance plan, and tracked throughout the life-cycle, until they are resolved and the product delivered.

4 Risk in Design and Development

Risk management in the implementation phase deals with avoiding knowable risks by using resources effectively in a balance of pro-active mitigation and contingency planning, and maintaining reserves to deal with the inevitable “unknown-unknowns.” To deal with risks across the board – technical and programmatic – performance, cost and schedule – we look at, use, and control the reserves. Not only dollars and schedule slack, but margins in spacecraft resources such as mass, power, processor memory, throughput, pointing error allocations, and so on may be used to mitigate risks, or reserved as liens against the occurrence of risks.

Figure 4 displays a life-cycle related margin utilization curve, illustrative of the thinking that margin is planned at the beginning, and its use is planned throughout the development, leaving, as appropriate for each resource, suitable reserve for use in operations. Systems engineering controls the distribution of reserves, using formulas derived from historical growth in resource usage. The JPL resource reserve policies are documented in the Design, Verification/ Validation and Operations (DVVO) Principles (Reference 1). Adding reserves for specific risks identified through the risk management process, the total reserve pool can then be judicially applied.



▲ Use JPL's "Design Verification, Validation, and Operations Principles in picking the milestone values

Figure 4 Margin Management

Risk as a Parameter in Systems Engineering Trade Studies

A powerful area of applying the risk assessment part of the RM process is to identify the risk parameters in design decisions and problem-solving processes, which are led by the systems engineers. The first element is to ask the design team to rigorously identify risks in the options under consideration. Using a discipline that asks “what is the condition that indicates a risk?”, then “what is the risk event you fear, and when?”, and finally, “what would be the consequence to the project?” pushes the analyst to identify as specific and measurable a risk as possible. Secondly, applying a standardized set of assessment criteria (i.e. the criteria adopted in the project RM plan), the team assessments can be normalized to compare apples with apples. Figure 5 shows the 5X5 matrix suggested for JPL projects to use.

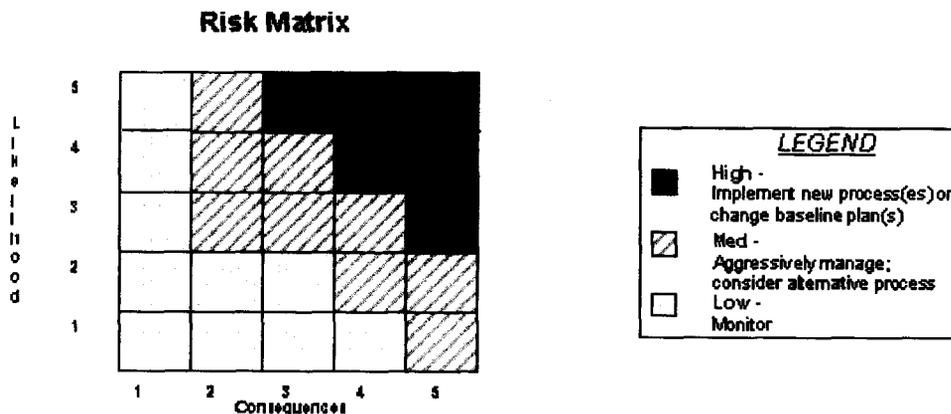


Fig 5 JPL Risk Management 5X5 Matrix

This matrix is almost identical to the 5X5 matrix used by the independent assessment teams at JPL and other NASA centers, but slightly tailored to provide utility over the entire life-cycle. This will be discussed more in the next section.

The criteria that define the 5 levels of likelihood and consequence for both mission risk and implementation risk are illustrated in fig 6.

Likelihood of Occurrence (Circle One)					
<u>Level</u>	<u>Level Definition</u>		<u>Level</u>	<u>Implementation Risk Level Definition</u>	
5	Very High	>70%, almost certain	5	Overrun budget and contingency cannot meet launch	
4	High	>50%, More likely than not	4	Consume all contingency, budget or schedule	
3	Moderate	>30%, Significant likelihood	3	Significant reduction in contingency or launch slack	
2	Low	>1%, Unlikely	2	Small reduction in contingency or launch slack	
1	Very Low	<1%, Very unlikely	1	Minimal reduction in contingency or launch slack	

Consequence of Occurrence (Circle one for each type checked above)		Consequence of Occurrence (Circle one for each type checked above)	
<u>Level</u>	<u>Mission Risk Level Definitions</u>	<u>Level</u>	<u>Implementation Risk Level Definition</u>
5	Mission failure	5	Overrun budget and contingency cannot meet launch
4	Significant reduction in mission return	4	Consume all contingency, budget or schedule
3	Moderate reduction in mission return	3	Significant reduction in contingency or launch slack
2	Small reduction in mission return	2	Small reduction in contingency or launch slack
1	Minimal (or no) impact to mission	1	Minimal reduction in contingency or launch slack

Fig 6 Assessment Criteria for 5X5 Matrix

The specific values or impact levels are not important to this discussion – in fact projects will adapt these to their needs. What is important is that a common set be applied to all of the process applications on the project – so far we have talked about initial planning, acquisitions, and systems engineering trades.

When the engineering decisions have been reached, two important elements of the systems engineering/ risk management integration will have been improved. First, risks assumed in the winning solution will be portable to the project risk list straightaway. Secondly, cost and schedule impacts of the design decisions will have been addressed, and the appropriate changes or liens adopted in the plan.

Mission Assurance Risk Assessments

Another area where Risk Management integrates into the Systems Engineering-like functions in the project implementation is the Risk Rating provided monthly by the Mission Assurance Manager (MAM) and his/her team on each project. These are reviewed by the Office of Safety and Mission Success (OSMS) management and thus are an in-house but independent risk assessment of the Assurance functions on the project. Fig 7 shows a typical matrix of areas assessed.

OSMS (61X)	MAM	System Safety	HQA	SQA	Conf. Mgmt.	Rel	Envrmt	Parts	Mat'ls & Proc	Cont. Control	Missio n Ops
---------------	-----	------------------	-----	-----	----------------	-----	--------	-------	------------------	------------------	-----------------

Fig 7 Safety and Mission Assurance Fever Chart

5 Risk in Verification, Validation, and Commitment

In the process on JPL Flight Projects called ATLO (Assembly, Test, Launch and Operations), the Risk Management process and the Commitment to Launch come together. Over the past decade, NASA and JPL have developed a significant risk assessment process involving systems engineering assessments, discipline-focused “red team” reviews, and Independent Assessment teams which are chartered by the NASA program codes to provide advice to the launch approval officials (most often the Associate Administrator (AA) for the affected Enterprise, but sometimes the Administrator). Various agencies within the NASA structure conduct these reviews. The Independent Program Assessment Office (IPAO) provides review capability and coordination. These teams sometimes report to the Administrator’s Program Management Council, and more often to the Enterprise AA. In addition, the Systems Management Office at each center provides teams who report their findings to the Center Governing Program Management Council (GPMC). In addition, OSMS conducts an Independent Mission Assurance Review (IMAR) for the NASA Safety and Mission Assurance Office, which covers all of the risk-related issues arising from the Mission Assurance work on the project. Fig 8 shows the agenda topics. Key features include a risk-rating of the Problem/ Failure Report (PFR) close-outs, and the degree of success in the planned Verification and Validation campaign.

With all these independent teams, the assessment of risk has been standardized to use the 5X5 Matrix mentioned earlier. In this phase of the life-cycle, the mission risk consequences are the focus of the assessments.

IMAR Agenda

- **MER-B Trajectory/Launch Window**
- **Incompressible Test List**
- **Operating Hours**
- **Project Safety Status**
- **Contingency Planning**
- **Operations Readiness and Training**
- **Problem Reports**
- **Waivers**
- **Special Topic: Single Point Ground Fuse Anomaly**
- **Special Topic: Spirit (MER-A) In-flight Performance**
- **Residual Risk List**
- **Mission Assurance Launch Readiness**

Fig 8 Typical IMAR Agenda

6 Conclusions

The growth and maturing of the risk management application at JPL is encouraging. The interfaces with the rest of the processes applied to flight projects still need improvement. In particular, it is very important that the interfaces with project and flight systems engineering be identified and instantiated, since systems engineering is the core activity defining and controlling the development of the product. In this paper, some of the current interfaces between risk management and system engineering, and systems engineering-like processes, have been discussed. Current promising integrated actions with risk-focus have been identified, and some areas with great promise of controlling and managing cost through risk-based systems thinking have been identified. The hope is that the importance of risk management and the need to apply its formal methodologies will continue to be emphasized by NASA and JPL management, such that the needed integration with the extant processes can be achieved.

ACKNOWLEDGMENT

The research described in this paper was carried out ^{at} ~~by~~ the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

References

- 1 “Design, Verification/Validation & Ops Principles for Flight Systems (Design Principles), Rev. 2”, JPL document D-17868, Mar 03, 2003

internal

BIO

Title of Paper: SPACE SYSTEMS ENGINEERING AND RISK MANAGEMENT –
JOINED AT THE HIP

Name: Dr. James R Rose
Position: Engineering Principle - Risk Management Process
Owner
Company: Jet Propulsion Laboratory (JPL) *Caltech* —
Degrees Received: BaSC – Engineering Physics – University of
Toronto
MS and PhD – Aeronautics – California Institute of
Technology
SE/RM Work Experience: 15 years – Spacecraft and Project Systems
Engineering – JPL Flight Projects (Mariner Mars
71, SEASAT), Advanced studies (Venus Orbiting
Imaging Radar, Mars Rover and Sample Return)
15 years – Project Systems Engineer – SP-100,
Talon Gold, TOPEX/ Poseidon)
7 years – Process Owner – Risk Management and
Reviews
Related SE and RM Expertise: Co-Author and Instructor for 10 years, Systems
Engineering 4-day course through Learning Tree
International.