

RISK BASED DECISION TOOL FOR SPACE EXPLORATION MISSIONS

Leila Meshkat, Steve Cornford, Terence Moran

Jet Propulsion Laboratory, California Institute of Technology
4800 Oak Grove Drive
Pasadena, CA 91109

ABSTRACT

This paper presents an approach and corresponding tool to assess and analyze the risks involved in a mission during the pre-phase A design process. This approach is based on creating a risk template for each subsystem expert involved in the mission design process and defining appropriate interactions between the templates. A separate "risk expert" mediates this process and incorporates the information obtained by the various subsystems to produce a report that reflects the weak links of the mission, the major risk elements for each phase, and the overall risk measure.

BACKGROUND

The Jet Propulsion Laboratory (JPL) employed the concept of concurrent engineering to create the Advanced Projects Design Team (Team X) in April 1995. This team produces conceptual designs of space missions for the purpose of analyzing the feasibility of mission ideas proposed by its customers. The customers often consist of principal investigators of design teams who aim to plan new mission proposals. The study takes one to two weeks and the design is then documented in a 30 to 80-page report that includes equipment lists, mass and power budgets, system and subsystem descriptions, and a projected mission cost estimate. The study is then reviewed and summarized and an abbreviated report is also produced.

The project design team consists of 20 engineers, each representing a different discipline, and a team leader. Table 1 shows the disciplines. The team leader coordinates and facilitates the mission design process and interacts with the customers to ensure that their objectives are properly captured and represented in the design.

Engineers are equipped with techniques and software packages used in their area of expertise and interact with the team leader and other engineers to study the feasibility of the proposal and produce the optimal design for their specific subsystem within their feasible region. Often, there are conflicting or competing objectives for various subsystems and many trade studies are conducted between subsystem experts in real time. Computers used by various team members are networked and there are also large screens for the display of information. Some of the communication between team members, however, happens in a face-to-face manner. Subsystems that need to interact extensively are clustered in close proximity to facilitate the communication process between the experts

Table 1: Team X Disciplines

Systems	ACS	Instrument	Mission Design
Telecom	Risk	Software	Programmatics
Thermal	Cost	Structures	Configuration
C&DH	EDL	Propulsion	Ground Systems
Science	Power	Logistics	Trajectory Vis

Often the design process starts with the articulation of the customer requirements and overall concepts by the team leader and the Systems expert. These engineers have met with the customer in a pre-session to discuss the study objective and define the required products. The mission is designed in an iterative manner. In each iteration, the following events take place sometimes sequentially and other times in parallel: The subsystem experts of Science, Instruments, Mission Design and Ground Systems collaboratively define the science data strategy for the mission in question. The Telecom, Ground Systems, and Command and Data Handling (C&DH) experts develop the data return strategy. Then, the Attitude Control Systems (ACS), Power, Propulsion, Thermal, and Structure experts iterate on the spacecraft

design and the Configuration expert prepares the initial concept. The Systems expert interacts with subsystems to ensure that the various subsystem designs fit into the intended system architecture. Each subsystem expert publishes design and cost information and the Cost expert estimates the total cost for the mission. Often at this point, the team iterates on the requirements and each subsystem expert refines or modifies design choices. This process continues until an acceptable design is obtained. This design is then documented and submitted to the customer.

MOTIVATION

The motivation for the work presented in this paper can be summarized as follows:

1. Provide a framework to enable the consideration of risk throughout the design process.
2. Produce better risk profiles for the mission to document in the report.
3. Facilitate better communication between the various subsystem experts.
4. Capture the information communicated between subsystem experts for future reference and decision traceability purposes.

It's important to note that the mission design sessions in question are very rapid and the design engineers are stretched for time. Therefore, it was crucial for us to develop an approach and corresponding tool that allows for meeting the above goals with minimal work on the side of the subsystem experts and minimal obstruction on their activities. Providing the capability to trace back and capture major decisions that are made throughout the process of a design session is the theme of an approach we presented in an earlier paper [1]. The main objective of the work addressed in this paper is to initiate a process for interacting with the team experts and obtaining information from them. The implementation of a tool to provide the capability described in [1] is not the primary focus and will be a follow on to this work. Moreover, the immediate needs of the team include the production of better risk profiles for the mission to be included in the reports and a framework for risk consideration during the design process. Therefore it is important for us to address those needs.

The main software framework used in the design sessions is Microsoft Excel©. In addition, each of the subsystem experts has their own

specialized tools. For example, the Configuration expert uses CAD/CAM packages to visualize and design the structure of the spacecraft, the Mission Design & Visualization expert uses tools such as SOAP© (Satellite Orbit Analysis Program) to design and display the trajectory, and the Software expert uses COCOMO© (CONstructive COSt MODEL) to modularize and cost the software in question. The "Cost" expert uses statistical methods and packages such as Monte Carlo simulation tools to allow for the determination of parametric cost curves for the missions. But it's important to note that the common tool used by all is Microsoft Excel and the underlying database for the team (ICEMaker©) interacts with the Excel workbooks.

Our tool, the "Risk Analysis Prototype" (RAP) requires interaction on the part of all the members of the team; therefore it was pretty clear that it had to be compatible with Microsoft Excel and display a similar user interface. The following section discusses our approach and the resulting architecture of the tool. In the Risk Analysis Prototype section, we show some snapshots of the tool, discuss its usage and show how the information generated using this tool helps us achieve the goals mentioned in this section. Section 5 talks about the conclusions of this paper and the future directions of the project.

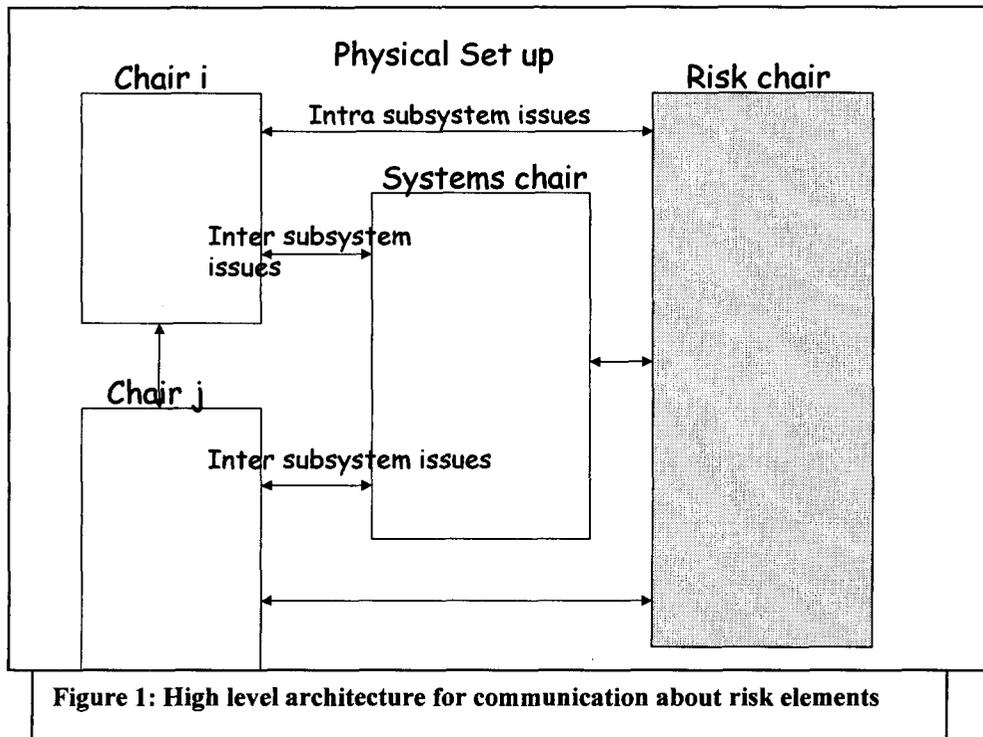
APPROACH

The approach we undertook for tackling this problem was to determine the minimal amount of information necessary to meet our goals and the least obtrusive method of obtaining it. Note again that the primary goal is to initiate a process that would allow us to interact with the domain experts via the tool and extract information from them.

We determine this minimal amount of information to be as follows: every subsystem expert (periodically throughout the design) identifies the main *risk elements*, a subjective measure of risk *likelihood* and *impact*, possible affected *objectives*, and potential *mitigations*. Further, we looked at the scope of various risk elements. If an element only affects one subsystem, we consider it to be an *intra-subsystem* issue. If, on the other hand, it affects more than one subsystem, it's an *inter-subsystem* issue. Figure 1 shows the main physical set up of the system and the communication protocol defined for the various types of risk elements.

Note that we include a Risk expert in the figure. Note that the terms “expert”, “subsystem” and “chair” are often used synonymously in Team X. This is the latest addition to the subsystems at the Project Design Center at JPL. The goal of the risk expert is to facilitate the process of risk capture and analysis within the team. As shown in the figure, the *intra-subsystem* risk elements, which affect only one subsystem, are directly communicated to the risk chair. The *inter-subsystem* elements, however, which affect more than one subsystem, are communicated with the Systems chair first. This is because any elements which affect more than one subsystem may affect each of them differently and the high level effect from the systems perspective should be assessed by the Systems expert.

subsystem to provide risk elements to other subsystems. One such mechanism has been built into RAP and will be described further in the following section. The subsystem designers, on the other hand, periodically view their risk spreadsheet for any items sent to them. The items can be either accepted and analyzed, or rejected and forwarded to other subsystems. In addition, subsystem experts can also add risk elements to their risk spreadsheet and determine the list of other subsystem experts who should be made aware. If an expert believes that a risk element only affects her own subsystem, she could declare it as “self-owned”, but still ask for her analysis to be relayed to other specified subsystem experts for information purposes.



PROCESS

Throughout the design session, the risk chair identifies the risk elements related to the various subsystems and distributes this information to the relevant experts. As we mentioned in the previous section, there are two types of risks, *inter-subsystem* and *intra-subsystem*. *Inter-subsystem* risks affect more than one subsystem, while *intra-subsystem* risks affect only one. Moreover, there needs to be a mechanism for one

If the expert has identified an element, which relates only to one other subsystem, she can simply “provide” it to the subsystem expert in question. If, on the other hand, an element relates to more than one subsystem, then the expert can declare it to be a “shared element” and send it to multiple subsystem experts. The Systems chair automatically receives any element declared as “shared” and is asked to analyze it from a systems perspective.

Risk Analysis Worksheet											Export to Word	
Study: Study Name		Update Interface								Overview Fever Chart		
Role: ACS												
Risk Element	Phase of Risks	Likelihood	Impact	Mitigations Applied	Mitigated Likelihood	Mitigated Impact	Affected Objective	Explanation	Source	Owner		
<input checked="" type="checkbox"/> Pointing Accuracy		1	1						ACS/Default	ACS		
Pointing Stability		4	4						ACS/Default	ACS		
Reliability		1	1	ok	4	4	this	is	ACS/Default	ACS		
<input checked="" type="checkbox"/> Meet bore sight knowledge requi		2	5	mits	4	4	ok	ok	ACS/Default	ACS		
Calibration relative to instrument		1	1	done	4	4			ACS/Default	ACS		
<input checked="" type="checkbox"/> New shared risk for Thermal c		1	1						Power/Provided	ACS		
<input checked="" type="checkbox"/> I removed an empty column an		1	1	ok	2	2	what		Power/Provided	ACS		
<input checked="" type="checkbox"/> there is no name field in the r		1	1	ha	1	1			Power/Provided	ACS		
edfg: edf		1	1						ACS/Novel	ACS		
edfg: edf		3	5						ACS/Novel	ACS		
dfgh		1	1	ok	5	5	what	dfgh	ACS/Novel	ACS		
ertert		3	4						ACS/Novel	ACS		
edfg: edf		2	5						ACS/Novel	ACS		
edfg: edf									ACS/Novel	ACS		
edfg: edf		3	5						ACS/Novel	ACS		

Figure 2: A snapshot of the RAP tool as it appears on the ACS system template

RISK ANALYSIS PROTOTYPE (RAP)

Figure 2 shows a snapshot of the RAP worksheet on the ACS system template. Each row represents a risk element along with its attributes. These attributes include the *phase*, *likelihood*, *impact*, *mitigations applied*, *mitigated likelihood*, *mitigated impact*, the *affected objective*, an optional *explanation*, the *source*, and the *owner*. Upon opening the template, the user can click on the button that indicates “Add Risk”. This is shown in Figure 3. A window pops up automatically. In this window, there’s a box where the user can type in the risk element. Further down, the user must indicate the risk to be either a risk for its own role, a provided risk element, or a shared risk element. If the user clicks on the button indicating “this is for my role”, it will only be reflected on the screen of the user’s subsystem and its source and owner attributes will be specified as the user’s subsystem. If the user clicks on the button indicating, “This is a risk for”, the next step would be choosing the subsystem to which the risk element must be sent on the menu that appears. In this case, the risk will be sent to the subsystem in question. On the spreadsheet for that subsystem, the source will be indicated to be the subsystem that provided

the risk and the owner will be the subsystem that received it. If the user specifies a risk to be a “shared risk”, then it will automatically be sent to the user in question, the Risk and Systems experts, and any other subsystems that the user specifies. Note that on the individual templates, the source will be the subsystem on the sending end and the owner will be the subsystem on the receiving end. After receiving a risk element, the subsystem expert can analyze it. Once the risk has been added, the user can either check the box that indicates “Analyze this risk now” or click on the button with the “fever” chart colors in front of the risk element in question. In both cases, a window pops up with the red, yellow and green “fever” chart and the user can click on the box that indicates the likelihood and impact of the risk in question. This is shown in Figure 4. Note that the attributes indicated in these pop-up windows can also be filled out manually in the Excel spreadsheets. Moreover, additional attributes such as the affected objective, mitigation, and explanations can also be filled out in the Excel spreadsheet. This framework allows the designer to tailor the level of information input based on personal preferences and/or time restrictions.

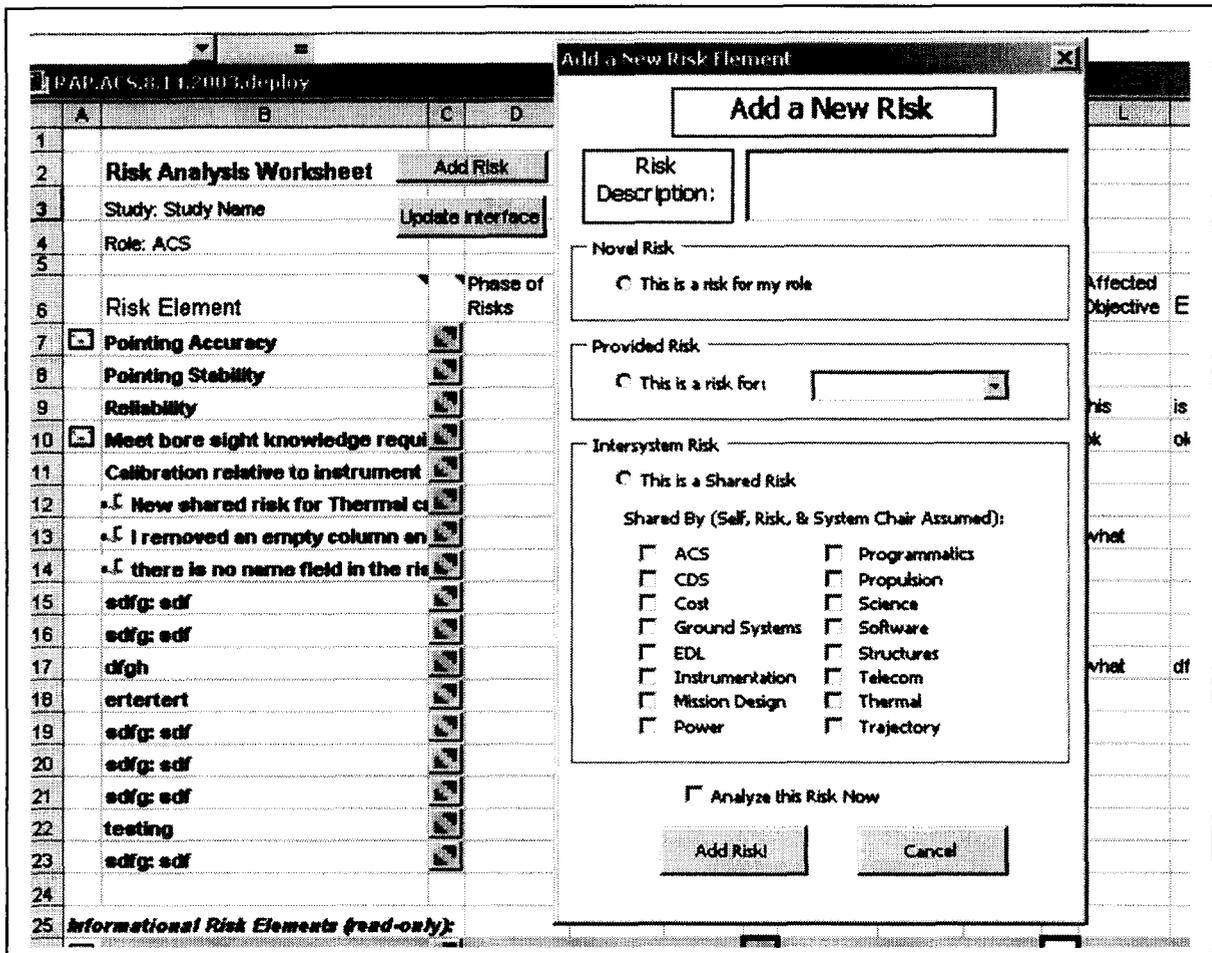


Figure 3: A snapshot of the RAP tool showing the “Add Risk” capability.

The buttons on the right hand side of Figure 2 show more capabilities of the RAP tool. By clicking on the “Export to Word” button, the tool automatically generates a report including a chart with dots indicating the risk items and a list of the items with their attributes. Users can automatically import this document to their reports. The three icons on the very right are “trash”, “instant messaging” and “lock” respectively. Clicking on the “trash” icon will delete the risk item. The “instant messaging” icon can be used for messaging back and forth about the risk item in question and the user can “lock” the element once the modifications are complete.

In addition to the information represented on the template, information about the instances of time when changes are made to the spreadsheets is

also stored in the database. Decisions are made throughout the design session with consideration of the risks, costs, and performance of the various options. Therefore capturing just the risk items, the objectives that they impact, and the domain expert’s assessment about their likelihood and impact levels along with the time and change history will enable us to trace back some of the major decisions.

Hence this tool allows us to capture information in a minimally obtrusive style. The information captured can be used to generate risk profiles for missions. These profiles will include the system level and subsystem level risks. The risk expert has the task of assessing the overall mission risk and using the information captured and the

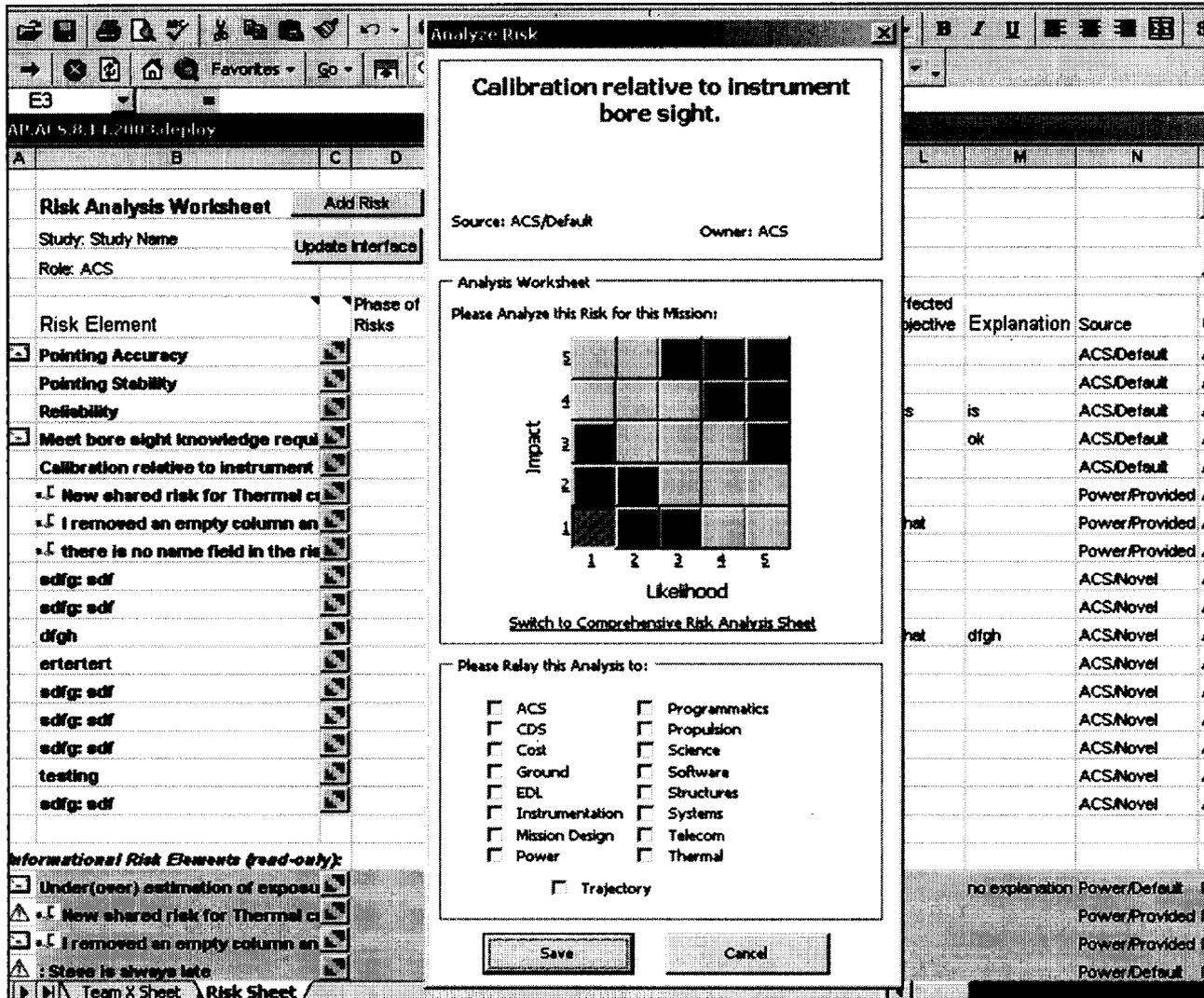


Figure 4: A snapshot of the RAP tool showing the “Analyze Risk” capability.

capabilities of the tool to finalize the risk report. The information captured can also be used for tracing back the thought processes of the designers throughout the design session. For instance, if a risk element is identified and then removed, this could indicate a different design decision. The same is true when a mitigation is suggested and then applied. If there is controversy among several subsystem experts about the likelihood or impact of a particular risk element on the same objective, this indicates that there needs to be future discussion on the issue to clarify matters. Hence effective communication among the subsystem experts is initiated and we are one step closer to “risk based design”.

CONCLUSIONS & FUTURE DIRECTIONS

This paper presents an approach and corresponding tool to assess and analyze the risks involved in a mission during the pre-phase A design process. The tool is easy to use and minimally obtrusive to the design engineers. Moreover, the information generated using this tools allows us not only to produce better risk profiles for the mission in question, but also to trace back some of the thought processes and decisions of the designers. This is a first step towards the realization of “risk based design” and “decision capture”.

Exploration and integration of tools and techniques for “risk based design” is the focus of the “Risk Tool Suite” which is being built as part of the NASA funded “Engineering for Complex Systems” program. One of these tools is “Defect Detection and Prevention” or DDP [2] which has been produced by NASA at JPL. In the future, we plan on creating the necessary link between RAP and DDP so that the information generated using RAP can be sent to DDP for more thorough analysis.

ACKNOWLEDGEMENTS

The authors would like to thank André Girerd for his laudable efforts in bringing this paper to publication. Such contributions are worthy of song.

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

References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement by the United States Government or the Jet Propulsion Laboratory, California Institute of Technology.

REFERENCES

[1] L. Meshkat, S. Cornford, M. Feather, “Traceability and Decision Capture in Semi-structured Contexts”. *Proceedings of the Fifteenth International Conference on Software Engineering & Knowledge Engineering (SEKE)*, San Francisco, California, USA, July 1-3, 2003, pp. 647-655

[2] M.S. Feather, S.L. Cornford, J. Dunphy & K. Hicks; “A Quantitative Risk Model for Early Lifecycle Decision Making”; *Proceedings of the Conference on Integrated Design and Process Technology*, Pasadena, California, June 2002. Society for Design and Process Science