

Towards a Systems Approach to Risk Considerations for Concurrent Design

Leila Meshkat, Robert E. Oberto

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

ABSTRACT

This paper describes the new process used by the Project Design Center at NASA's Jet Propulsion Laboratory for the identification, assessment and communication of risk elements throughout the lifecycle of a mission design. This process includes a software tool, "RAP" that collects and communicates risk information between the various designers and a "risk expert" who mediates this process. The establishment of this process is an attempt towards the systematic consideration of risk in the design decision making process. Using this process, we are able to better keep track of the risks associated with the design decisions. Furthermore, it helps us develop better risk profiles for the studies under consideration. We aim to refine and expand the current process to enable more thorough risk analysis capabilities in the future.

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.

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

Table 1: Team X Disciplines

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 information provided by the customers usually includes the proposal team objectives, the science and technology goals, the mission concept, initial take on necessary payload & associated spacecraft and mission design, the task breakdown between providers of parts or functions, top challenges and concerns and approximate mission timeline. This information is often provided electronically in a format accessible to the designers and is partially presented by the customer representatives during the initial session.

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 engineers find a feasible conceptual design for a space mission to satisfy the customer requirements very rapidly. There are various modeling tools and techniques available to them for performing the necessary analyses. But ultimately many of the design decisions are based on expert opinions and there isn't sufficient time in the rapid design timescale for exploring the full option space. Rather, the team identifies a point design that satisfies the mission requirements. This is partially due to the fact that the

existing high fidelity models are mostly at the subsystem level and the interrelationships between the different subsystems are not fully captured at the systems level.

Design decisions are made with consideration of risk, cost and performance. In addition, the implication of decisions made by one subsystem engineer on the option space of other subsystems and the ripple effects are also discussed throughout the session. These discussions often occur concurrently during the sessions. At times when major trades are being considered, the related subsystem engineers have breakout sessions to discuss them and come to a consensus. Due to the numerous dependencies that exist between the various subsystems in a spacecraft, and the speed with which the engineers make design decisions, it sometimes happens that the subsystem engineers are unaware of some important design choices of others. Since each design option correlates with particular types of risks, one way of keeping the engineers informed about the design options being considered is by informing them about the risks related to them dynamically. This is one of the motivations for the work described in this paper.

We classify the types of missions studied in TeamX based on the goals of the customers. These goals include identifying the feasibility of a particular design within the indicated cost caps, comparing various architectures for a given set of high level requirements, re-costing or reviewing missions that are designed in other teams or studying the implications of using new technologies. In each of these cases, risk plays a fundamental role. In the case of feasibility studies, it is important to understand the risks involved in implementing the design. For comparisons between various architectures, risk is one of the discriminators. One of the major concerns in using new technologies is the risks that they might impose. Moreover, it is important that we keep good track of risks identified in earlier portions of study throughout the entire process.

In summary, the motivation for the work presented in this paper is as follow:

1. Providing a framework to enable systematic consideration of risk throughout the design process.
 - a. Consideration of risk by means of identification, communication and assessment of particular risk elements.
2. Facilitating better communication between the various subsystem experts.
3. Providing a means for keeping experts informed about the latest design decisions and their relevant risk measures during the sessions.
4. Providing better risk profiles for the mission to document in the report that is produced for the customers.
5. Capturing the information communicated between subsystem experts for future reference and design decision traceability purposes.

APPROACH

1. Overview

Our approach consists of two main parts: the tool and the process. On one hand, we designed, developed and implemented a distributed software tool to enable communication of the risk items and their related attributes. On the other hand, we defined a common risk dictionary for use by the team and developed a process for conducting risk assessment in the team. Training the team to use the tool & dictionary consistently during the mission design process to identify, assess and communicate the risk items is an ongoing effort. An overview of our approach is shown in Table 2. Initially, we defined the risk dictionary and iterated on it with the team. The team also helped us identify the software requirements; they included the ease of use and the interoperability with the Excel spreadsheets on which the whole software infrastructure is built. It was necessary for our process to be as minimally obtrusive as possible, due to the fact that the design sessions are intense and there is very limited time for additional work. The next step involved the design of the architecture for building the tool and the initiation of the process of “risk training” within the team. We iterated on the risk-related definitions and terms with the team members. Furthermore, the risk expert discusses the risk items implied by the design decisions with the individual engineers to facilitate the communication between them during the design sessions.

STEP ONE:	STEP TWO	STEP THREE	FUTURE STEPS
<ul style="list-style-type: none">•Define Risk Terminology;•Define software requirements	<ul style="list-style-type: none">•Design Architecture for Software tool•Initiate Process of “risk training” within team	<ul style="list-style-type: none">•Develop prototype tool.•Train team members to use tool and refine tool using team feedback.•Determine role of risk chair/ approach for risk communication within team.	<ul style="list-style-type: none">•Use tool concurrently during design.•Build standard risk item libraries to make consistent assessments across missions.•Refine tool•Add additional features;•Towards Probabilistic Risk Assessment in Conceptual Design

Table 2: Overview of approach for establishing risk assessment process in TeamX.

In the following section, we discuss the software tool and the experimental results obtained to date from using the tool in the team.

2. Risk & Rationale Assessment Program (RAP)

The RAP software tool is a distributed system that enables the communication between various designers using a Microsoft Excel interface. Figure 1 shows a screenshot of the RAP user interface. Once the RAP tool is installed on the computer, it can be initiated by

pressing the button “New RAP sheet” that appears on the Excel toolbar. Then the user is given a menu of “studies”, “roles” and “user-names”. Once the user picks from that menu, the screen shown in figure 1 appears. In this screen, the study name is “Test” and the role “Risk”. The user defines new risk elements by pressing on the “New Risk” button on the toolbar. This initiates the “New Risk Element” box shown in figure 1. The user then fills in the information about the risk and identifies the affected subsystems. In order to assess the risk, the user clicks on the fever chart button that appears next to the risk element title on the table. This is shown in figure 2.

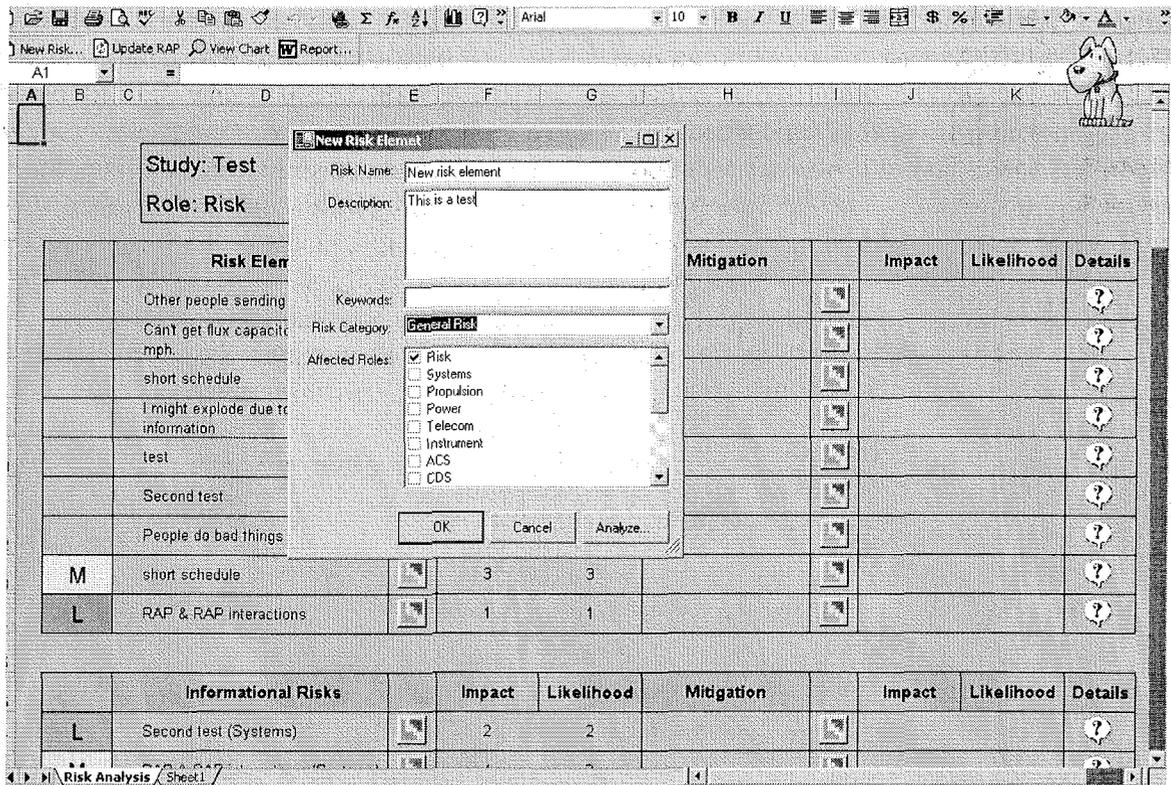


Figure 1: RAP screenshot showing the “New Risk Element” initiation process.

The second table shown on the user interface includes the attributes of the “Informational Risks”. These are the same risks that the user in question initiated and sent to other subsystems by indicating their roles as being affected by them. The user can view the assessment of these risks by those subsystem experts and any information that they’ve included in their assessments by looking into the various attributes

The second fever chart button next to the “Mitigation” column collects information about possible mitigations and an assessment of the risk item in question after the mitigation has been applied. The users can indicate a mitigation to be “applied” or “suggested”. In cases where mitigation is suggested, but not applied, it doesn’t affect the residual risk of the item. Pressing on the “details” button on the right hand side column can capture other kinds of descriptions and/or explanations about the item. The information is communicated through a centralized database. The users click on the “Update Interface” button on the toolbar to send or receive information from the database.

The tool also provides the users with the capability to view the global risk profile for the mission at any point during the design process. By clicking on the “view chart” button on the toolbar, the user’s can access the fever chart shown in figure 3. By selecting the roles of interest, the user can see the risk elements associated with those roles on the fever charts. Clicking on the subsystem acronyms on the chart then provides the user with the detailed information about the risk items associated with the subsystem.

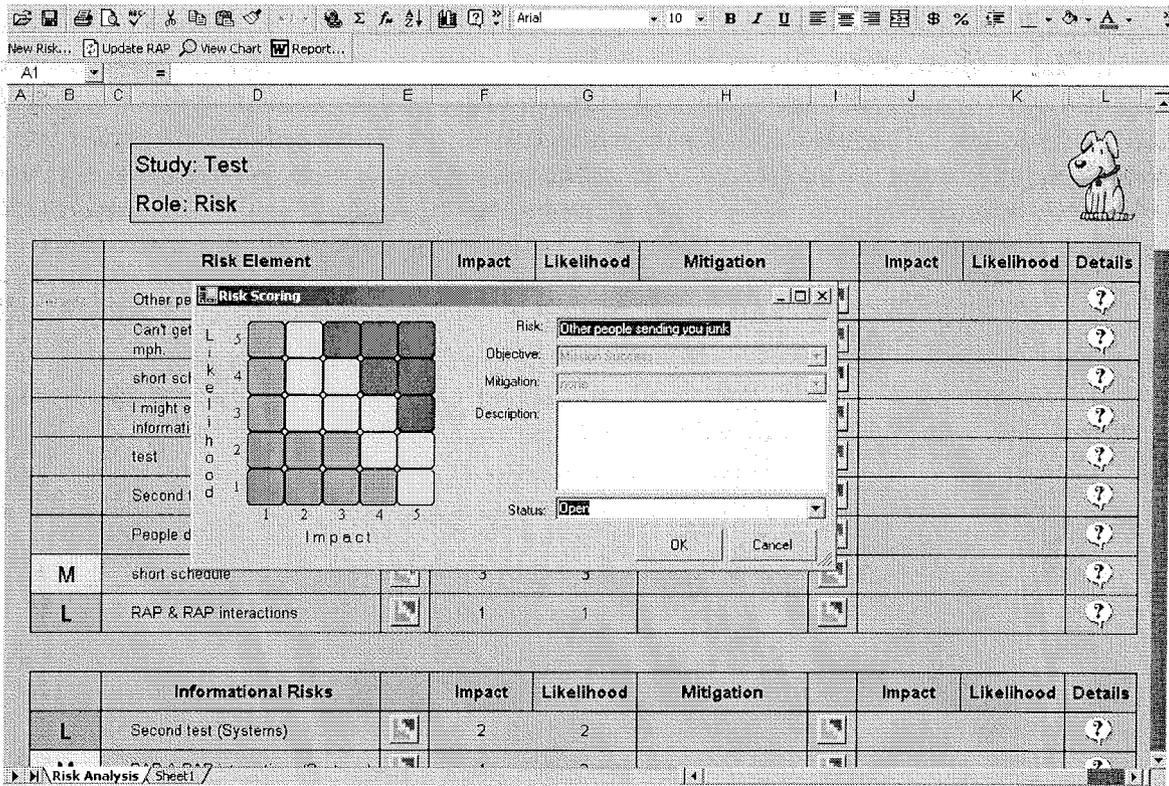


Figure 2: RAP screenshot showing the “Risk Scoring” process.

Finally, the tool has the capability of generating automated “Risk reports” based on information available on the spreadsheets. By clicking on the “Report” button on the toolbar, a report is generated in Microsoft Word. This report includes the fever chart, a table with all the risks as assessed by various subsystem engineers and an appendix including all the details about each of the risk items.

3. Experimental Results

The risk assessment process & tool explained earlier is currently being used in the team. It has been used for the risk assessment of numerous studies. These studies include “red team reviews” which are the most rapid type of study conducted in TeamX. Their time span is usually one full day and during this time the team reviews a preliminary design provided by the customer. The process helps the designers to communicate their risk items and keep on top of the design decisions made by other designers. It also helps develop better risk profiles for the missions.

between these entities. Therefore the next step for us is to expand the capabilities of the tool to enable the capture of these entities along with their relationships. In addition, we are currently exploring the application of other risk assessment tools and techniques, for providing more elaborate risk models. We collaborate with the NASA sponsored Engineering for Complex Systems programs in integrating the RAP tool within the “Risk Tool Suite for Advanced Design” tool suite. This tool suite provides an environment that allows for the seamless transfer of data between various risk modeling tools including the most popular probabilistic risk assessment (PRA) tools. In addition to the data collected using RAP, we consider the data available from the TeamX customers and the data generated during the sessions for conducting PRA studies for the missions.

REFERENCES:

[1] *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, version 1.1, prepared for the Office of Safety and Mission Assurance, NASA HQ, Washington, DC, August 2002.

ACKNOWLEDGEMENTS:

We would like to acknowledge Luke Voss, the developer of the RAP software.

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.

Towards a Systems Approach to Risk Considerations for Concurrent Design

Leila Meshkat, Robert E. Oberto

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

ABSTRACT

This paper describes the new process used by the Project Design Center at NASA's Jet Propulsion Laboratory for the identification, assessment and communication of risk elements throughout the lifecycle of a mission design. This process includes a software tool, "RAP" that collects and communicates risk information between the various designers and a "risk expert" who mediates this process. The establishment of this process is an attempt towards the systematic consideration of risk in the design decision making process. Using this process, we are able to better keep track of the risks associated with the design decisions. Furthermore, it helps us develop better risk profiles for the studies under consideration. We aim to refine and expand the current process to enable more thorough risk analysis capabilities in the future.

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.

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

Table 1: Team X Disciplines

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 information provided by the customers usually includes the proposal team objectives, the science and technology goals, the mission concept, initial take on necessary payload & associated spacecraft and mission design, the task breakdown between providers of parts or functions, top challenges and concerns and approximate mission timeline. This information is often provided electronically in a format accessible to the designers and is partially presented by the customer representatives during the initial session.

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 engineers find a feasible conceptual design for a space mission to satisfy the customer requirements very rapidly. There are various modeling tools and techniques available to them for performing the necessary analyses. But ultimately many of the design decisions are based on expert opinions and there isn't sufficient time in the rapid design timescale for exploring the full option space. Rather, the team identifies a point design that satisfies the mission requirements. This is partially due to the fact that the

existing high fidelity models are mostly at the subsystem level and the interrelationships between the different subsystems are not fully captured at the systems level.

Design decisions are made with consideration of risk, cost and performance. In addition, the implication of decisions made by one subsystem engineer on the option space of other subsystems and the ripple effects are also discussed throughout the session. These discussions often occur concurrently during the sessions. At times when major trades are being considered, the related subsystem engineers have breakout sessions to discuss them and come to a consensus. Due to the numerous dependencies that exist between the various subsystems in a spacecraft, and the speed with which the engineers make design decisions, it sometimes happens that the subsystem engineers are unaware of some important design choices of others. Since each design option correlates with particular types of risks, one way of keeping the engineers informed about the design options being considered is by informing them about the risks related to them dynamically. This is one of the motivations for the work described in this paper.

We classify the types of missions studied in TeamX based on the goals of the customers. These goals include identifying the feasibility of a particular design within the indicated cost caps, comparing various architectures for a given set of high level requirements, re-costing or reviewing missions that are designed in other teams or studying the implications of using new technologies. In each of these cases, risk plays a fundamental role. In the case of feasibility studies, it is important to understand the risks involved in implementing the design. For comparisons between various architectures, risk is one of the discriminators. One of the major concerns in using new technologies is the risks that they might impose. Moreover, it is important that we keep good track of risks identified in earlier portions of study throughout the entire process.

In summary, the motivation for the work presented in this paper is as follow:

1. Providing a framework to enable systematic consideration of risk throughout the design process.
 - a. Consideration of risk by means of identification, communication and assessment of particular risk elements.
2. Facilitating better communication between the various subsystem experts.
3. Providing a means for keeping experts informed about the latest design decisions and their relevant risk measures during the sessions.
4. Providing better risk profiles for the mission to document in the report that is produced for the customers.
5. Capturing the information communicated between subsystem experts for future reference and design decision traceability purposes.

APPROACH

1. Overview

Our approach consists of two main parts: the tool and the process. On one hand, we designed, developed and implemented a distributed software tool to enable communication of the risk items and their related attributes. On the other hand, we defined a common risk dictionary for use by the team and developed a process for conducting risk assessment in the team. Training the team to use the tool & dictionary consistently during the mission design process to identify, assess and communicate the risk items is an ongoing effort. An overview of our approach is shown in Table 2. Initially, we defined the risk dictionary and iterated on it with the team. The team also helped us identify the software requirements; they included the ease of use and the interoperability with the Excel spreadsheets on which the whole software infrastructure is built. It was necessary for our process to be as minimally obtrusive as possible, due to the fact that the design sessions are intense and there is very limited time for additional work. The next step involved the design of the architecture for building the tool and the initiation of the process of “risk training” within the team. We iterated on the risk-related definitions and terms with the team members. Furthermore, the risk expert discusses the risk items implied by the design decisions with the individual engineers to facilitate the communication between them during the design sessions.

STEP ONE:	STEP TWO	STEP THREE	FUTURE STEPS
<ul style="list-style-type: none">•Define Risk Terminology;•Define software requirements	<ul style="list-style-type: none">•Design Architecture for Software tool•Initiate Process of “risk training” within team	<ul style="list-style-type: none">•Develop prototype tool.•Train team members to use tool and refine tool using team feedback.•Determine role of risk chair/ approach for risk communication within team.	<ul style="list-style-type: none">•Use tool concurrently during design.•Build standard risk item libraries to make consistent assessments across missions.•Refine tool•Add additional features;•Towards Probabilistic Risk Assessment in Conceptual Design

Table 2: Overview of approach for establishing risk assessment process in TeamX.

In the following section, we discuss the software tool and the experimental results obtained to date from using the tool in the team.

2. Risk & Rationale Assessment Program (RAP)

The RAP software tool is a distributed system that enables the communication between various designers using a Microsoft Excel interface. Figure 1 shows a screenshot of the RAP user interface. Once the RAP tool is installed on the computer, it can be initiated by

pressing the button “New RAP sheet” that appears on the Excel toolbar. Then the user is given a menu of “studies”, “roles” and “user-names”. Once the user picks from that menu, the screen shown in figure 1 appears. In this screen, the study name is “Test” and the role “Risk”. The user defines new risk elements by pressing on the “New Risk” button on the toolbar. This initiates the “New Risk Element” box shown in figure 1. The user then fills in the information about the risk and identifies the affected subsystems. In order to assess the risk, the user clicks on the fever chart button that appears next to the risk element title on the table. This is shown in figure 2.

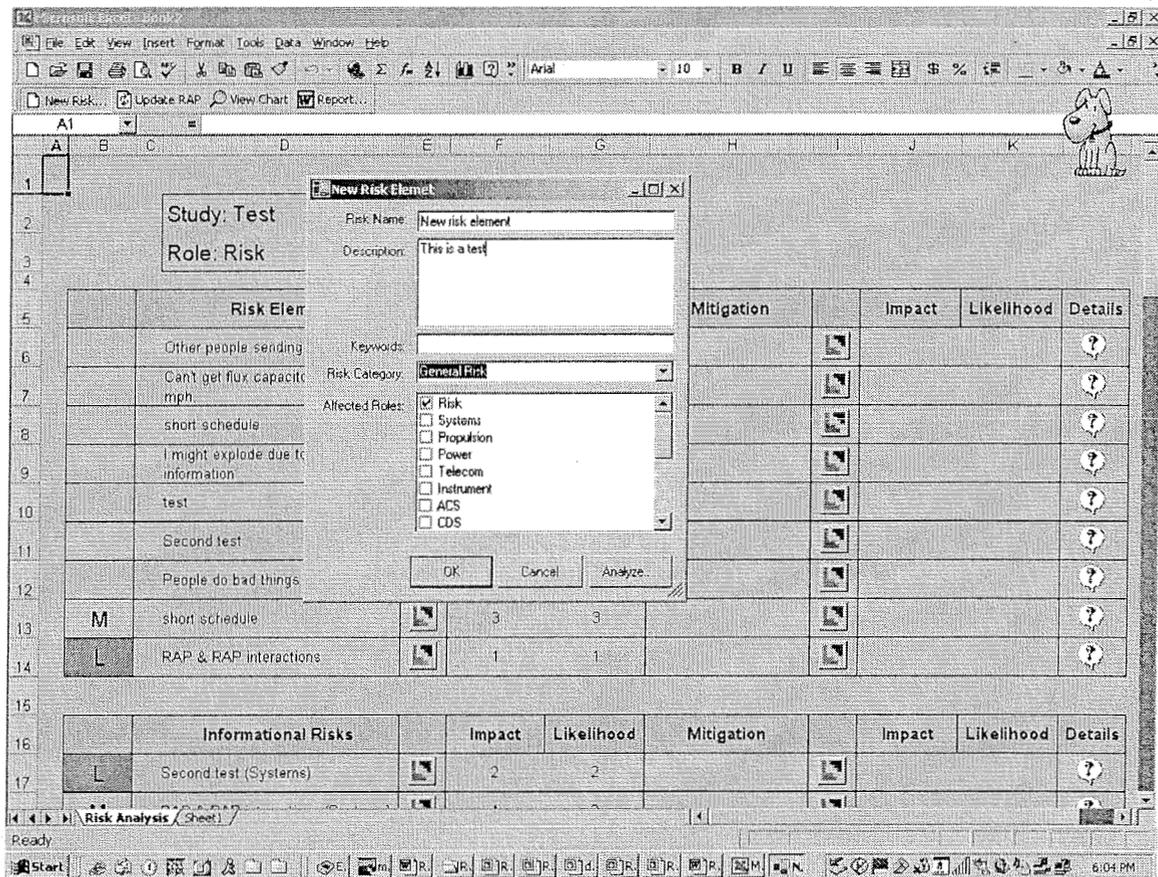


Figure 1: RAP screenshot showing the “New Risk Element” initiation process.

The second table shown on the user interface includes the attributes of the “Informational Risks”. These are the same risks that the user in question initiated and sent to other subsystems by indicating their roles as being affected by them. The user can view the assessment of these risks by those subsystem experts and any information that they’ve included in their assessments by looking into the various attributes

The second fever chart button next to the “Mitigation” column collects information about possible mitigations and an assessment of the risk item in question after the mitigation has been applied. The users can indicate a mitigation to be “applied” or “suggested”. In cases where mitigation is suggested, but not applied, it doesn’t affect the residual risk of the item. Pressing on the “details” button on the right hand side column can capture other

kinds of descriptions and/or explanations about the item. The information is communicated through a centralized database. The users click on the “Update Interface” button on the toolbar to send or receive information from the database.

The tool also provides the users with the capability to view the global risk profile for the mission at any point during the design process. By clicking on the “view chart” button on the toolbar, the user’s can access the fever chart shown in figure 3. By selecting the roles of interest, the user can see the risk elements associated with those roles on the fever charts. Clicking on the subsystem acronyms on the chart then provides the user with the detailed information about the risk items associated with the subsystem.

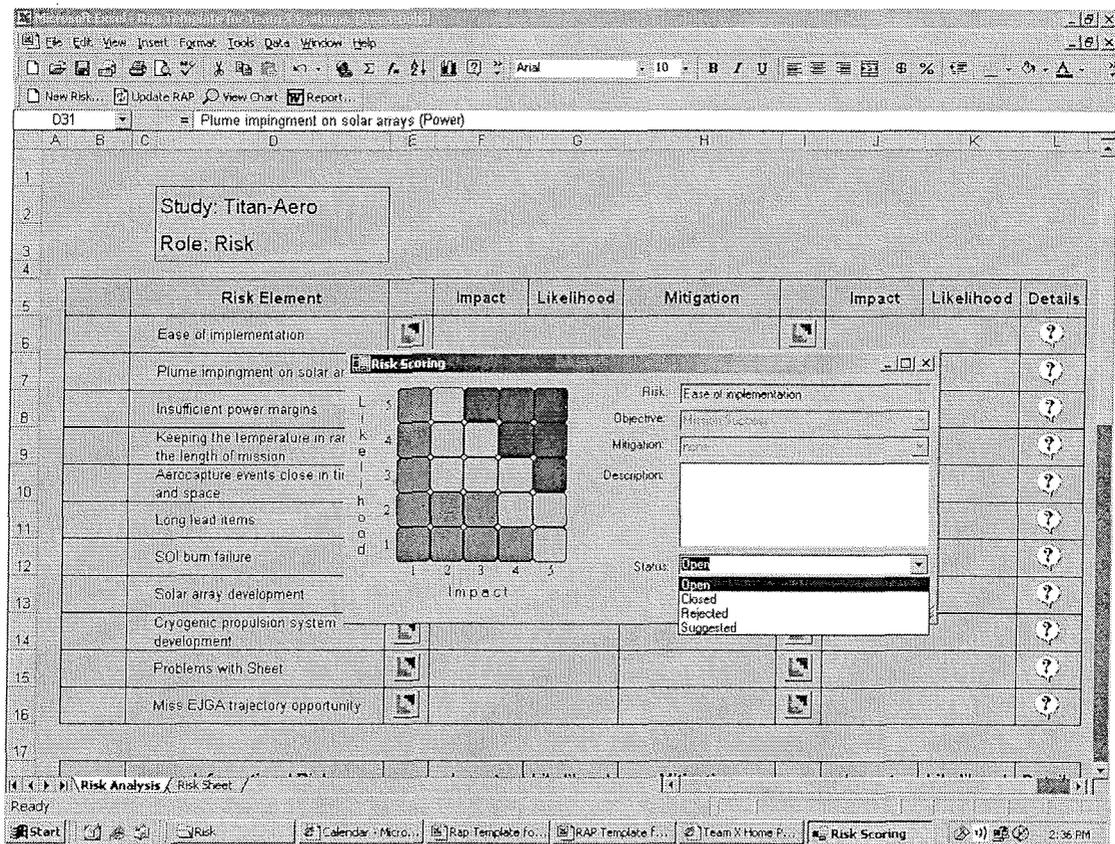


Figure 2: RAP screenshot showing the “Risk Scoring” process.

Finally, the tool has the capability of generating automated “Risk reports” based on information available on the spreadsheets. By clicking on the “Report” button on the toolbar, a report is generated in Microsoft Word. This report includes the fever chart, a table with all the risks as assessed by various subsystem engineers and an appendix including all the details about each of the risk items.

3. Experimental Results

The risk assessment process & tool explained earlier is currently being used in the team. It has been used for the risk assessment of numerous studies. These studies include “red team reviews” which are the most rapid type of study conducted in TeamX. Their time

span is usually one full day and during this time the team reviews a preliminary design provided by the customer. The process helps the designers to communicate their risk items and keep on top of the design decisions made by other designers. It also helps develop better risk profiles for the missions.

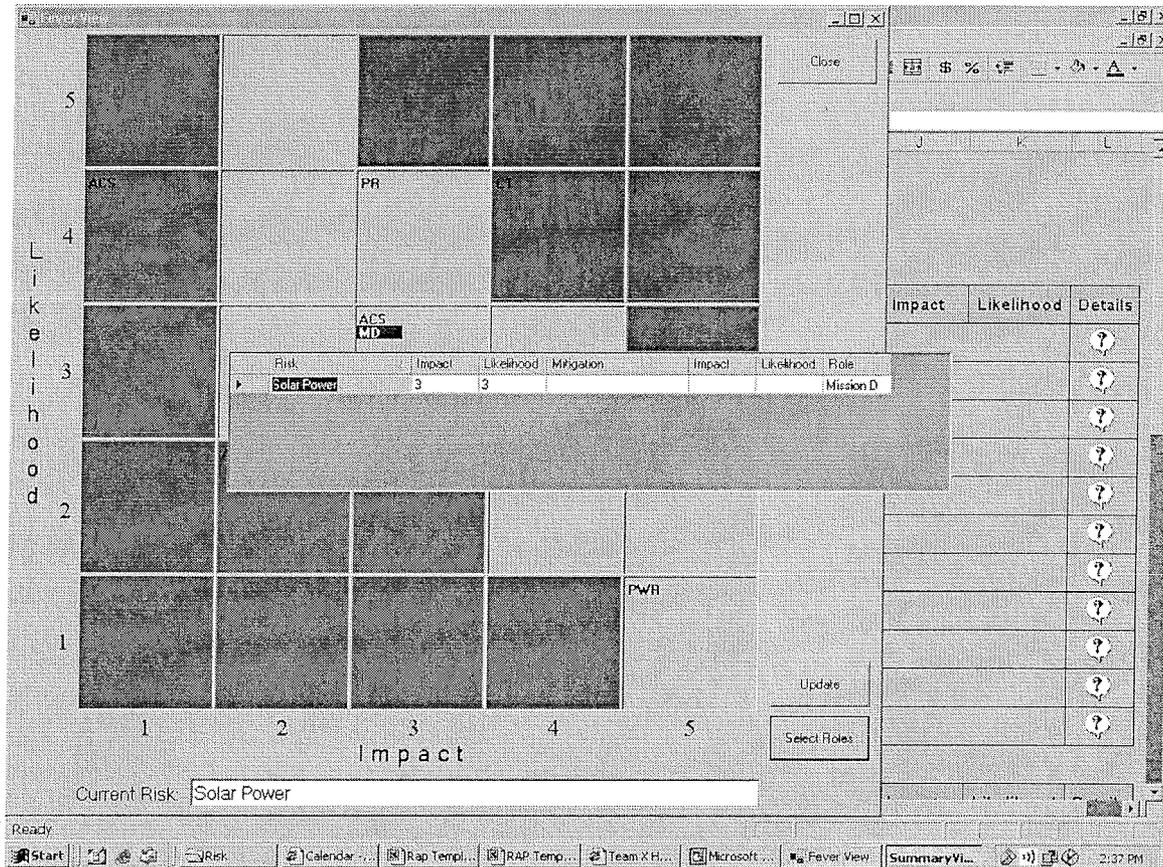


Figure 3: RAP screenshot showing the global fever chart.

FUTURE DIRECTIONS

We plan on expanding the process in two directions: the operation in the team and the addition of analytical capabilities. Each of these is discussed below:

1. Operation

We plan on moving the operation of the risk process forward to the point where it becomes a seamless part of the TeamX process. This will be accomplished as the process is refined incrementally and the experts become more comfortable with it.

Currently, the experts mostly use the tool after they have identified the final design for their subsystems. While this is useful in and of itself, it would be even more useful to identify the risks as options are considered for the design. This would help keep track of the risk during the process of design decision making.

2. Towards Probabilistic Risk Assessment (PRA)

Failures occur due to a combination of events that happen in a particular order within a given context. One main goal in conducting risks studies is to predict the possible failure scenarios and their respective likelihoods in order to avoid them. For this purpose, it is necessary to capture other entities in addition to risk elements. These entities include assumptions, events and contexts. It is also necessary to determine simple relationships between these entities. Therefore the next step for us is to expand the capabilities of the tool to enable the capture of these entities along with their relationships. In addition, we are currently exploring the application of other risk assessment tools and techniques, for providing more elaborate risk models. We collaborate with the NASA sponsored Engineering for Complex Systems programs in integrating the RAP tool within the “Risk Tool Suite for Advanced Design” tool suite. This tool suite provides an environment that allows for the seamless transfer of data between various risk modeling tools including the most popular probabilistic risk assessment (PRA) tools. In addition to the data collected using RAP, we consider the data available from the TeamX customers and the data generated during the sessions for conducting PRA studies for the missions.

REFERENCES:

[1] *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, version 1.1, prepared for the Office of Safety and Mission Assurance, NASA HQ, Washington, DC, August 2002.