

AN INTEGRATED APPROACH TO RISK ASSESSMENT FOR CONCURRENT DESIGN

Leila Meshkat, Luke Voss, Martin Feather, Steve Cornford
Jet Propulsion Laboratory
California Institute of Technology
4800 Oak Grove Drive
Pasadena, CA 91109

Abstract

This paper describes an approach to risk assessment and analysis suited to the early phase, concurrent design of a space mission. The approach integrates an agile, multi-user risk collection tool, a more in-depth risk analysis tool, and repositories of risk information. A JPL developed tool, named RAP, is used for collecting expert opinions about risk from designers involved in the concurrent design of a space mission. Another in-house developed risk assessment tool, named DDP, is used for the analysis.

The risk model in DDP is generated by integrating the information collected in RAP, other design information available from the design sessions, and possibly risk and failure information available from other libraries and databases. The underlying software infrastructure for this transfer of information is based on translating the RAP data to XML, which in turn is interpreted by DDP and translated to DDP data. The advantage of the integration is its combination of the strengths of the components, while avoiding the need to construct a single monolithic all-encompassing tool and process.

We briefly describe each of the RAP and DDP tools and demonstrate the integrated approach with an example generated from a study conducted at the Project Design Center (TeamX) at JPL.

1. 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	Program-matics
Thermal	Cost	Structures	Configuratio n
C&DH	EDL	Propulsion	Ground Systems
Science	Power	Logistics	Trajectory Visualization

Table 1: TeamX 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.

2. Introduction

In this section, we provide a brief introduction to the Risk and Rationale Assessment Program (RAP) and Defect Detection and Prevention (DDP) risk assessment tools.

2.1 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.

The second table shown on the user interface includes the attributes of the "Informational Risks". These are the same risks that the user in

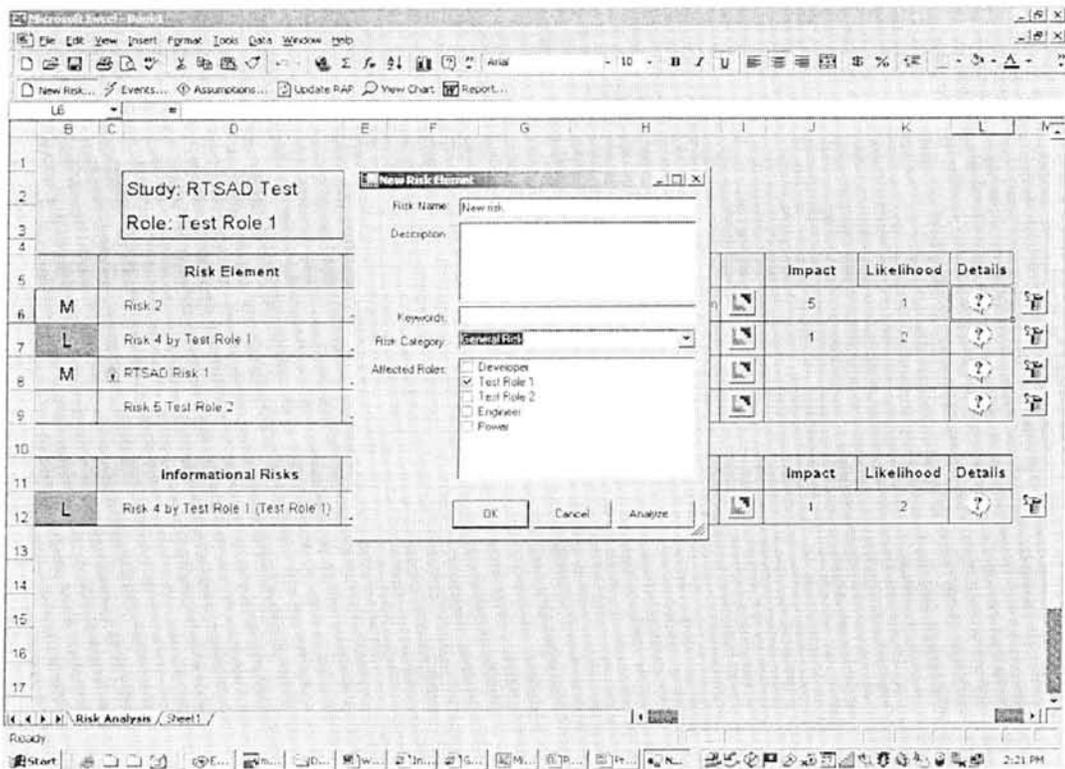


Figure 1: RAP screenshot showing the “New Risk Element” initiation process.

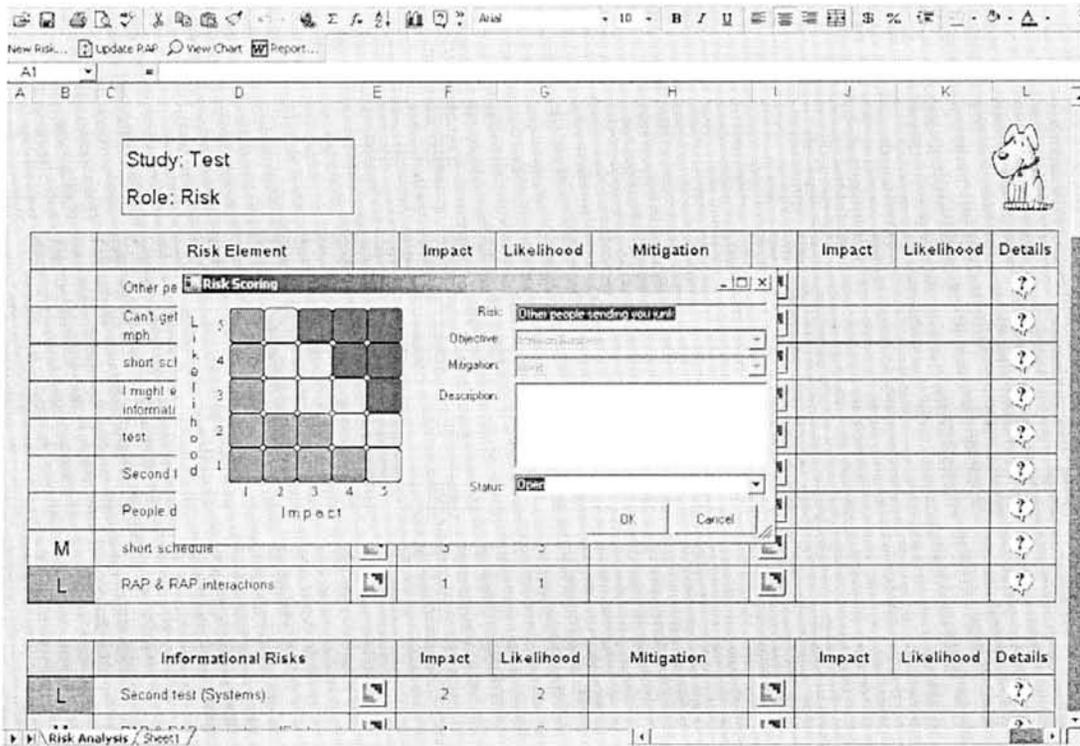


Figure 2: RAP screenshot showing the “Risk Scoring” process.

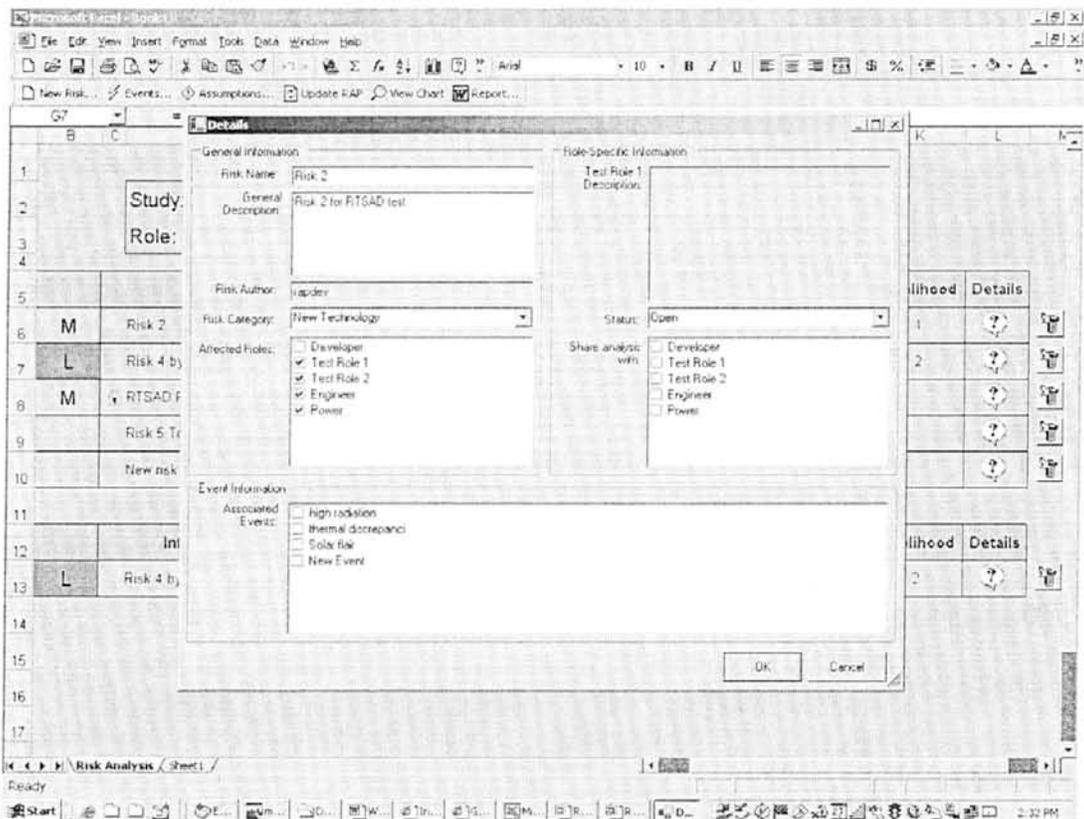


Figure 3: RAP Screenshot showing the “Details” for risk element “Risk2”

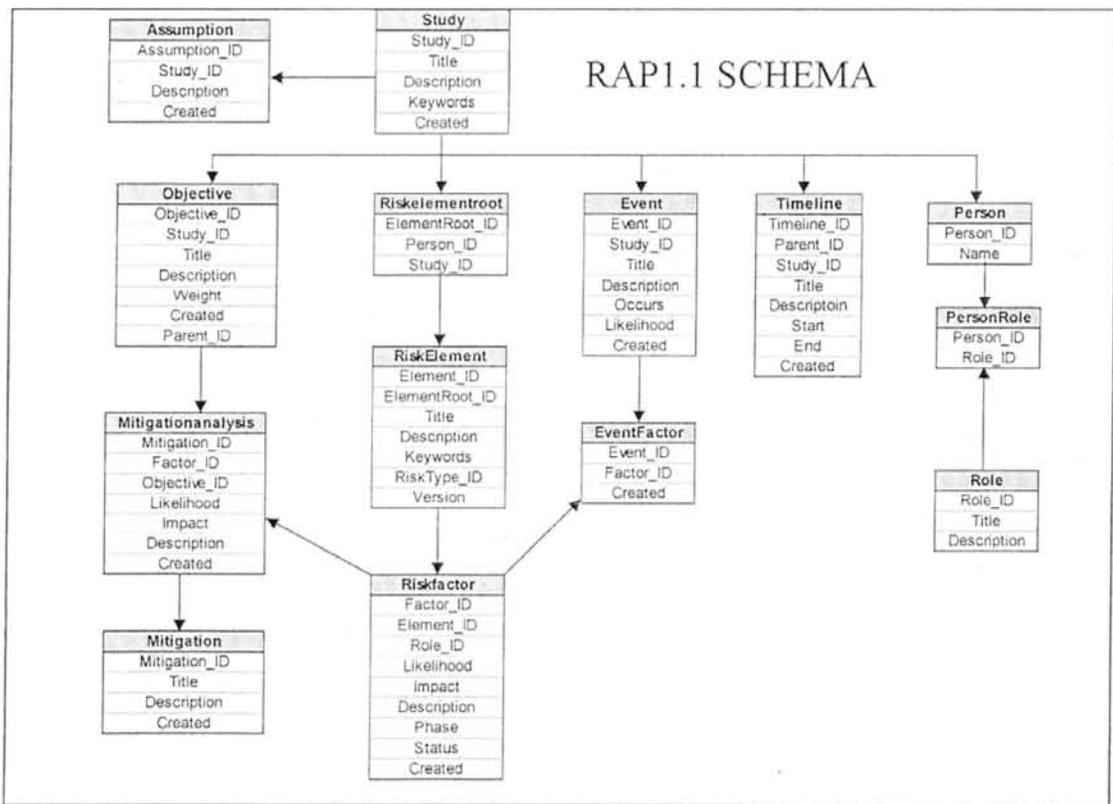


Figure 4: The underlying RAP Schema

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.

In addition, users can specify the "Events" associated with the mission and correlate them with the risk elements. The events are identified by clicking on the "Events" button on the toolbar, and adding the event of interest. Once an event is added, it appears on the event list. The events can then be correlated with the risk elements, by clicking on the details button on the risk element row. The details of risk element "Risk2" are shown in figure 3. In the bottom table on the pop up box, there is a screen with all the events listed on it. Users can pick any number of these events, and thus correlate them with the risks in question. This features facilitates the collection of expert opinions for the purpose of conducting Probabilistic Risk Assessment studies [3], [4].

Probabilistic Risk Assessment is a scenario based methodology. Scenarios are strings of events that begin with an initiator and lead to some sort of a conclusion, or end state. In between the initiator and end state are pivotal

events in the scenario. Pivotal events may either be protective, mitigative, aggravative, or benign. Scenarios can be modeled in many different fashions, but are most commonly modeled through the use of event trees and fault trees. The best way to describe the difference between event trees and fault trees is that event trees show the logical progression of events, while fault trees are snapshots in time, and are used to model events in the event tree.

Event trees are said to be based on inductive, or forward, logic; i.e., the forward thinking represents the possible conditional events in the scenario based on the preceding event, or the possible events that can occur given an initiator. Fault trees are said to be deductive in nature, i.e., they are used to identify all of the possible failure causes of an event from a top down approach. There is no one single way to develop a PRA model and the trade off is that the larger the event tree, the smaller the fault trees, and vice versa. The use of event trees and fault trees and their sizes is up to the analyst, but their sizes are typically decided based upon the PRA methodology used (large event tree versus small event tree), and to facilitate defining a complex world with competing risks into a model with binary decision points.

RAP 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. 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.

Finally, RAP 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.

The underlying software schema for RAP is shown in figure 4. This schema has been designed to be consistent with other risk analysis tools; these tools include system level modeling tools such as DDP (explained in the next section), and tools used for Probabilistic Risk Assessment (PRA), such as QRAS, Galileo ASSAP, CAFTA, or SAPHIRE [3], [4].

2.2 Defect Detection and Prevention

“Defect Detection and Prevention” (DDP), is a simple risk model designed for application early in the lifecycle, when information is sparse yet the capability to influence the course of the development to follow is large. Cornford originally conceived of DDP specifically to facilitate assurance planning [9]. The core idea of DDP is to relate three sets of information:

1. “Objectives” (what you want to achieve).
2. “Risk Elements” (what can get in the way of attaining those objectives).
3. “Investments” (what you can choose to do to overcome the problems).¹

In DDP, relationships between these items are *quantitative* (e.g., *how much* a Risk Element, should it occur, detracts from an Objective’s attainment). Such a quantitative treatment is key to DDP’s realization of the vision of “risk as a resource”, as espoused in [11]. This is one of the key ways that DDP differs from many of the purely qualitative approaches (e.g., QFD [10]) usually employed early in the life cycle.

¹ In previous papers on DDP these three sets of information were referred to as “Requirements”, “Failure Modes” and “PACTs” respectively. The switch of terminology reflects application of DDP to areas more broad than implementation phase assurance planning. Investments refer to all of the possible activities that can detect, prevent (reduce probability of occurrence) and alleviate (reduce impact of occurrence).

Cornford’s initial experiments used Microsoft Excel® spreadsheets to manually explore the utility of the process. Positive results then led to development of custom software for the DDP process [1]. Supported by this software, DDP has been applied to assess the viability of, and planning for, the development of novel technologies and systems for use on space missions [6],[7].

The core steps of a DDP risk study are:

1. Represent the success requirements of the spacecraft mission as DDP’s “Objectives”. User-provided weightings indicate the relative importances of these.
2. Represent the plethora of all kinds of risks that could impede attaining those objectives as DDP’s “Risk Elements”. These can encompass a wide range of concerns: programmatic, technical, infrastructure, management and resources.
3. Capture the extent to which each Risk Element, should it occur, would detract from attainment of each Objective. These become DDP’s quantitative “impact” links. Note that multiple Risk Elements, to varying degrees, can impact an Objective, and similarly a Risk Element can impact multiple Objectives.
4. Represent the options for reducing risk, including preventative measures, development-time tests and analyses (which, by revealing the presence of problems, allow for their correction prior to flight), as DDP’s “Investments”. Each of these has associated resource costs (e.g., dollars, time, map, power). Investments may include technology investments, design/architectural options, tests, analyses, process controls, and operational solutions.
5. Capture the extent to which each Investment, should it be applied, would reduce each Risk Element. These become DDP’s quantitative “effect” links. Note that multiple Investments, to varying degrees, can effect a Risk

Element, and similarly an Investment can impact multiple Risk Elements.

6. Select Investments that together cost-effectively reduce Risks (thereby leading to attainment of the Objectives).

The DDP tool supports these steps. Its GUIs help users to enter, organize and edit the various kinds of information (Objectives, Effects, etc.). Quantitative calculations are performed automatically. For example, the magnitude of a Risk Element is computed as the product of its likelihood of occurrence (taking into account the reducing effects of investments) and its impact (sum of its impacts on the individual objectives). The overall purpose of DDP is to allow users to understand the often-complex interrelationships between Risks, Objectives and Investments, so as to guide their judicious selection of Investments. Further, it provides an optimization scheme that determines the optimal combination of Investments to employ for attaining a balance of risk and cost based on the preferences and constraints established by the decision maker.

Mission design using DDP is in fact an interactive process, sketched in Figure 1. Fundamental requirements are the starting point. The objectives of the project and lower level requirements are derived from these fundamental requirements. The events that can lead to the non-fulfillment of the objectives or the risk elements are then identified. Design choices are made to reduce the identified risks. These design choices, in turn, may introduce new risks and/or derived objectives. Therefore the mission design process is more cyclic than hierarchical and it takes a few cycles to refine the initial design and produce an acceptable design. The mission design process is dynamic in nature, and the flexibility of DDP is critical to easily capturing these refinements and modifications as the design matures.

In particular, one of the most powerful aspects of the DDP process is the explicit inclusion of the investments that can be used to reduce the likelihood and/or impact of the various risk

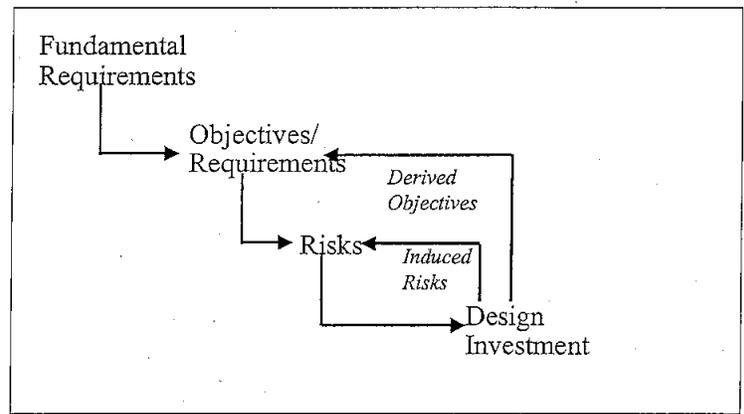


Figure 5: Requirements Flow Down and Ripple Effects of Option elements. The users can now explicitly examine the planned activities to ensure they are focused on the right elements of the design and explore various combinations of activities to mitigate the risks. Each of these investments has resource costs (e.g., mass, cost, power) associated with them and the tool provides a running total of the resources allocated to various investments. The DDP tool has been used as a front-end to provide quick, near real-time identification of a prioritized risk element list as well as the most promising investments. The tool allows the users to identify areas for additional work and it is this feature which will be exploited to identify areas most benefiting from more detailed, PRA analysis.

4. Integrated Approach

Using the data collected in RAP, we can generate risk profiles to supplement the study reports. However, RAP does not have any kind of analysis capability; it merely serves as a vehicle for collecting expert opinions and facilitating risk communication during the design sessions. Nevertheless, the data collected through RAP can be used to generate risk models using other types of tools.

In particular, the information generated in RAP can be input to DDP for further investigation. Note that the RAP schema includes risk elements, which are connected to Objectives and Mitigations. This corresponds with the DDP ontology. Automatic import of the RAP data to DDP is achieved by converting the RAP data to XML format and transfer into DDP. Figure 6 shows a screenshot of the DDP

model generated using information that was collected in RAP.

5. Conclusions & Future Directions

We recently conducted a case study in risk modeling using information generated in TeamX through RAP. This information was transferred to DDP, and using DDP we identified the vulnerabilities of the system. Further, we conducted a detailed analysis of the vulnerable parts of the system using the Galileo Dynamic Fault tree solution tool. In addition, we are in the process of building QRAS models which include event sequence diagrams. We are currently in the process of finalizing and synthesizing the results of this study.

7. Acknowledgements

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.

8. References:

- [1] M.S. Feather, S.L. Cornford, M. Gibbel. "Scalable Mechanisms for Goals Interaction Management", *Proceedings 4th IEEE International Conference on Requirements Engineering*, Schaumburg, Illinois, 19-23 Jun 2000, IEEE Computer Society, pp 119-129.
- [3] NASA's Third Workshop for Probabilistic Risk Assessment Methods (PRAM-3) for Managers and Practitioners, given at the Embassy Suites Hotel, Arcadia, California, June 3-6, 2002.
- [4] *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.
- [5] *Reactor Safety Study*, Report WASH-1400, Nuclear Regulatory Commission, 1975.
- [6] S.L. Cornford, J. Dunphy, and M.S. Feather: "Optimizing the Design of end-to-end Spacecraft Systems using risk as a currency",

IEEE Aerospace Conference, Big Sky, Montana, 2002

[7] S.L. Cornford, M.S. Feather & K.A. Hicks. "DDP – A tool for life-cycle risk management", *Proceedings, IEEE Aerospace Conference*, Big Sky, Montana, Mar 2001, pp. 441-451.

[8] S.L. Cornford, M.S. Feather, J.C. Kelly, T.W. Larson, B. Sigal & J.D. Kiper: "Design and Development Assessment", *Proceedings, 10th IEEE International Workshop on Software Specification and Design*, San Diego, California, 5-7 Nov 2000, pp 105-204.

[9] S.L. Cornford: "Managing Risk as a Resource using the Defect Detection and Prevention process", *Proceedings, 4th International Conference on Probabilistic Safety Assessment and Management*, 13-18 September 1998, New York City, NY, International Association for Probabilistic Safety Assessment and Management.

[10] Y. Akao. "Quality Function Deployment", Productivity Press, Cambridge, Massachusetts, 1990.

[11] M.A. Greenfield "Risk Management: 'Risk As A Resource'"
<http://www.hq.nasa.gov/office/codeq/risk/>.

[12] L. Meshkat, R.E. Oberto, "Towards a Systems Approach for Risk Considerations during Concurrent Design", *United Nations Space Conference, Beijing, China*, May 2004

[13] L. Meshkat, L. Voss, "Risk Based Decision Tool for Space Exploration Missions- Part 2", AIAA Space Conference, Fall 2004 - presentation made at the conference.

Figure 6: Screenshot of the DDP model generated using data collected through RAP.

