Probabilistic Risk Assessment for Concurrent, Conceptual Design of Space Missions

Leila Meshkat

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

ABSTRACT

NASA is expanding its capability to perform PRA. This capability gives insight into the weak links of a suggested design and drives the refinement of the design by identifying optimal areas for investments. Clearly, it is more viable and less expensive to refine a design at the time that it is being conceived. Hence the utility of conducting PRA at the conceptual design phase.

Concurrent engineering teams greatly reduce the design time and costs. However, there is currently no standardized means for building probabilistic risk models to assess risks associated with a design produced by such teams. The capability to produce a consistent and valid risk metric associated with such designs would greatly enhance the value of such design teams.

This paper explains the experimental results obtained to date from building probabilistic risk models for sample studies conducted at the concurrent engineering design team at the Jet Propulsion Laboratory (TeamX).

1. BACKGROUND

1.1 The Project Design Center (TeamX)

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 (usually involving 3-hour collaborative sessions) 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. There have been over 100 to date. More detailed information about TeamX can be found in [5] and [6].

1.2 Probabilistic Risk Assessment

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, aggregative, or benign. Scenarios can be modeled in many different fashions, but are most commonly modeled through the use of fault trees and event 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. Dynamic fault trees [8] extend the capabilities of traditional fault trees to represent the failure behavior of the system that is related to the order or sequence in which events occur. Phased mission dynamic fault trees [9] can model the sequence of mission phases.

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. The Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners [7] includes detailed information about PRA as applicable to space missions.

2. PRA IN TEAMX

2.1 *Motivation*

PRA has typically been performed on detailed design for verification purposes. Detailed design includes information about the exact components used in each of the subsystems of the spacecraft. Nevertheless, PRA doesn't need to be performed at the component level. The framework allows for the flexibility of its application at multiple levels of fidelity. Moreover, some of the most important design decisions are conducted at the conceptual design phase. At this phase, it is more viable and less expensive to refine a design. PRA during conceptual design can help identify optimal areas for investments of further analysis.

More recently, Fragola & Putney [1] developed a "Lego-Block" approach for updating pre-existing shuttle developed PRA models and associated data sets to analyze new launcher functions. The "Lego-Block" model includes a functional decomposition of the shuttle, and the blocks represent the various functions. These blocks are reconstructed and extended to alternative vehicles by experienced experts within reasonable time and resource constraints.

The increasing significance of probabilistic risk assessment in the context of a TeamX like environment is reinforced by the appearance of new suggested approaches in the recent literature [2, 10, and 11].

2.2 *Risk Assessment in TeamX*

The process used routinely for risk assessment in the TeamX allows for the identification, assessment and synthesis of the risk items perceived during the design process. The risk chair is responsible for identifying the relevant risk items and communicating them to the relevant experts using a distributed software tool, RAP [5]. Each of the experts, in turn, assesses the risks sent to them, and adds any additional risks they perceive in their design. Engineers deliberate on the risk items, and come to a consensus about their relative significance during the sessions. The risks are then synthesized into an overall risk report after deliberations in the team.

3. EXPERIMENTS

3.1 Mars Aerocapture PRA

The objective of the study conducted in TeamX was to provide the customer the necessary information to enable them to build a probabilistic risk assessment model for aerocapture at Mars. This model would be used for comparing the risks of different types of Mars orbit insertion, namely, aerocapture, aerobraking, and propulsive capture. The team considered several previously designed missions for Mars Sample Return that used Aerobraking and propulsive as the means for orbit insertion, and made the necessary changes for an Aerocapture study. Throughout the design sessions, the team members expressed their expert opinions about the significant assumptions, and events, and the risk elements along with their severity and correlation to the events. Also, per the customer's request, the discipline experts provided schematics of their subsystem designs and responded to specific questions posed by the customers. In particular, the PRA team had identified several major risk elements for aerocapture that the team elaborated upon. These risk elements included:

•Navigational delivery errors/entry angle
•Aeroheating and thermal loads
•Thruster capability to react to aerodynamic demands used to control capture (ACS)
•GN&C
•Atmospheric variability at Mars
•Separation interface for aeroshell

Because the customer's objective was to build a Probabilistic Risk Assessment (PRA) model based on this design, the design team members made an extra effort to generate the information necessary for conducting the PRA. This information was mainly captured through RAP (Risk & Rationale Assessment Program), which is the tool used in TeamX for risk data collection, communication, and synthesis. This data was then used for building risk models with several different risk modeling tools. These tools included the Defect Detection & Prevention tool (DDP), the Galileo ASSAP dynamic fault tree solver, the Quantitative Risk Assessment System (QRAS). The models built with these tools each serve a different purpose. We initially built a system level model using DDP. Analyzing this model helped us identify the vulnerable parts of the system. QRAS models were built to demonstrate the possible scenarios and sequences of events that lead to them, and test possible mitigations. Later, we built dynamic fault trees for the vulnerable system modules to analyze them further.

The programs that were used throughout the course of the case study to create risk models were:

1. Risk & Rationale Assessment Program (RAP)
2. Defect & Detection Prevention (DDP)
3. Quantitative Risk Assessment System (QRAS)
4. Galileo Dynamic Fault Tree solution software (Galileo)

Each risk analysis program had a unique role in producing the PRA of the case study.

RAP is a tool used by the members of TeamX to collect and synthesis expert opinions on risk. The approach for collection and assessment of risk-related information is described in [5].

DDP is a tool [12, 13] used to build broad models of the system. This model structures the mission information in terms of an objective tree, a risk tree and a mitigation tree, and the numeric dependencies between the different elements of each of these trees.

QRAS is one of the main Probabilistic Risk Assessment (PRA) tools [6] on the market. This tool produces event trees and their correlation with risk elements in the system. The QRAS models provide a visual representation of the mission hierarchy.

Galileo dynamic fault tree solution software generates dynamic fault trees of the system architecture [15]. The Galileo models give us insight into the subtle dependencies within the system, and the vulnerable elements at both a quantitative and qualitative level. The dependencies within the system can be observed in the graphical representation of these fault trees. The reliability of the subsystem can be computed by allocating failure rates to each of the components and running the model.

Detailed information about this case study can be found in [13].

3.2 Mars Odyssey and Mars Telecomm Orbiter

The goal of the Mars Odyssey (MO) study in TeamX was to adopt the existing Mars Odyssey design in the subsystem templates and use some recently introduced modeling techniques within the team environment to experiment with refining the existing design. During the first week, the main task was to use all the available information about the Mars Odyssey project to build the related design into the TeamX spreadsheet. Independently from TeamX, we had built risk models for this project using the Galileo Dynamic Fault Tree analysis tool as part of a project for assessing the robustness of the Mars Relay Network. More information about this study will appear in [16]. It turns out that the team study was very effective in helping us update the pre-built risk models and refining them accordingly. More specifically, the team helped us better assess the criticality of the failure of various components or subsystems. In some occasions, they suggested possible work arounds that could prevent the system failure. This information made us realize that many of the failures will result in degraded states, but not mission failure. In addition, since our risk models are extremely sensitive to the expert opinions and the expert interpretation of the failure information, obtaining more expert opinions was useful for updating the risk information.

The Mars Telecom Orbiter (MTO) design was developed by TeamX and the study report was available to us. This study looked at multiple options for the propulsion system and the launch date as well. In addition, it included information about some of the unique features that were being considered for the orbiter. These features were an Orbiting Sample Capsule, and a Rendezvous and Autonomous Navigation experiment. The report also included a risk report which listed and ranked some of the major risk items identified during the study. We used this information, along with information obtained from the project Mission Assurance Manager to develop risk models for this orbiter.

4. LESSONS LEARNED

The experiments described in the previous section gave us a better understanding about the utility of probabilistic risk assessment in a TeamX like environment, and the utility of a

TeamX like environment for conducting PRA studies.

On one hand, it became clear that TeamX provides an optimal environment for the review and verification of existing risk models. Therefore, one of the utilities of TeamX is for risk "red team reviews". On the other hand, we realized that TeamX can be used for generating a creative list of events, assumptions and risks associated with a design that can be used for generating PRA models after the fact. Our underlying software tool, RAP allows for the identification of events and assumptions, and for linking the events with the risk items. The events identified by the team members were very creative and different from those typically included in PRA studies. Therefore we realized that involving the entire design team in determining the elements of a PRA study helps generate out of the box information. Since one of the main challenges in any PRA study is the determination of the events and the failure modes of the system elements in the presence of these events this can provide considerable benefit.

The different design sessions conducted in TeamX are classified based on the target body (e.g. Mars, Moon, and Earth Science) and the type of mission (e.g. Science, Technology). There is significant overlap in the functions the spacecraft needs to perform, and the main events it encounters during each class of mission. Therefore, it's possible to build high level reference PRA models for each class of mission, and update them during the timeframe of a study (which is usually a week) to include some risk information in the report.

Currently, in TeamX, many design decisions are made on the fly and optimized through verbal discussions and expert assessments by the individual designers. In order to be able to exercise any kind of risk model, even pre-existing ones, it' necessary to make changes to the design process to accommodate the extra time and effort it takes to run these models. This extra time and effort relates to collecting the necessary information from the team members , tweaking the pre-canned models to represent this information, running it to generate results, and finally discussing the results with the team so they consider it as input to their decision making process.

Another important piece of information is the data that is used for exercising the models. Our experiments demonstrate the sensitivity of our results to even the expert interpretation of the objective failure data. In order to get consistent results across the different studies, it's important to use consistent data sets. This is often a problem in TeamX, because the risk information is mainly generated from expert opinions and the experts are not necessarily the same for the different studies. This problem can be mitigated as we generate a larger library of risk information.

5. CONCLUSIONS & FUTURE DIRECTIONS

The main conclusions of this study can be summarized as follow:

1. In order to build PRA models in real time, it's necessary to start with a reference PRA for a similar type of mission and refine as you go along.
2. TeamX can be used for verifying existing risk models using designer expert opinions.
3. Design and risk information generated during the TeamX session can be used for building PRA models after the design session.

Following are some of our plans for further infusion of PRA in the TeamX environment:

1. Continue building reference PRA's for the different classes of missions studied in TeamX.
2. Experiment with these reference PRA's in the real time design sessions.
3. Utilize the TeamX environment for PRA red team reviews.
4. Utilize the TeamX environment for generating the design and risk information for building PRA models after the fact.

6. 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.

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.

7. REFERENCES

[1] J. Fragola & Bl. Putney, "A Risk Evaluation Approach for Safety in Aerospace Preliminary Design',

[2] H. McManus, D. Hastings, and J. Warmkessel, "New Methods for Rapid Architecture Selection and Conceptual Design", *Journal of Spacecraft and Rockets, Vol 41, No. 1, January-February 2004.*

[3] N. Smith and S. Mahadevan, "Probabilistic Methods for Aerospace System Conceptual Design" *Journal of Spacecraft and Rockets, Vol. 40, No. 3, May-June 2003*

[4] J. Chachere, J. Kunz, and R. Levitt, " Observation, Theory and Simulation of Integrated Concurrent Engineering: Risk Analysis Using Formal Models of Radicl Project Acceleration, *CIFE Working Paper # WP088, August 2004, Stanford University*

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

[6] Mark, G. (2002). Extreme collaboration. *Communications of the ACM. Vol. 45(6), pp.89-93*

[7] *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.

[8] Joanne Bechta Dugan, Salvatore Bavuso, and Mark Boyd. "Dynamic fault tree models for fault tolerant computer systems." In *IEEE Transactions on Reliability*, 41(3), September 1992, pp. 363 - 377.

[9] L. Meshkat, L. Xing, S. Donohue & Y. Ou An Overview of the Phase Modular Fault Tree Approach to Phased Mission System Analysis;; *Proceedings of the Space Mission Challenges for Information Technology (SMC-IT 2003)*, Pasadena, CA July 13-16 2003

[10] J.L. Benjamin, and M.E. Pate-Cornell, "Risk Chair for Concurrent Design Engineering: Satellite Swarm Illustration", *Journal of Spacecraft and Rockets, Vol. 41, No. 1, 2004, pp. 51-59.*

[11] A. Farhang Mehr & I. Tumer " A New Approach to Probabilistic Risk Analysis in Concurrent and Distributed Design of Aerospace Systems" *Proceeeings of IDETC/DAC, Sep. 24-26 2005, Long Beach, CA.*

[12] 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.

[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.

[14] Kevin J. Sullivan, Joanne Bechta Dugan and David Coppit, *"The Galileo Fault Tree Analysis Tool,"* Proceedings of the 29th International Conference on Fault-Tolerant Computing (FTCS-29), 1999.

[15] J. Scherbenski, L. Meshkat, "A Case Study for Risk Assessment & Modeling inConceptual Concurrent Design" JPL Technical Report.

[16] L. Meshkat, A. Girerd, C.Edwards, "An Integrated Approach for the Probabilistic Risk Assessment of the Mars Relay Network", to be published in the *Proceedings of the Reliability & Maintainability Symposium, January 2006*

Probabilistic Risk Assessment for Concurrent, Conceptual Design of Space Missions

Leila Meshkat

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

ABSTRACT

NASA is expanding its capability to perform PRA. This capability gives insight into the weak links of a suggested design and drives the refinement of the design by identifying optimal areas for investments. Clearly, it is more viable and less expensive to refine a design at the time that it is being conceived. Hence the utility of conducting PRA at the conceptual design phase.

Concurrent engineering teams greatly reduce the design time and costs. However, there is currently no standardized means for building probabilistic risk models to assess risks associated with a design produced by such teams. The capability to produce a consistent and valid risk metric associated with such designs would greatly enhance the value of such design teams.

This paper explains the experimental results obtained to date from building probabilistic risk models for sample studies conducted at the concurrent engineering design team at the Jet Propulsion Laboratory (TeamX).

1. BACKGROUND

1.1 The Project Design Center (TeamX)

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 (usually involving 3-hour collaborative sessions) 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. There have been over 100 to date. More detailed information about TeamX can be found in [5] and [6].

1.2 Probabilistic Risk Assessment

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, aggregative, or benign. Scenarios can be modeled in many different fashions, but are most commonly modeled through the use of fault trees and event 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. Dynamic fault trees [8] extend the capabilities of traditional fault trees to represent the failure behavior of the system that is related to the order or sequence in which events occur. Phased mission dynamic fault trees [9] can model the sequence of mission phases.

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. The Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners [7] includes detailed information about PRA as applicable to space missions.

2. PRA IN TEAMX

2.1 *Motivation*

PRA has typically been performed on detailed design for verification purposes. Detailed design includes information about the exact components used in each of the subsystems of the spacecraft. Nevertheless, PRA doesn't need to be performed at the component level. The framework allows for the flexibility of its application at multiple levels of fidelity. Moreover, some of the most important design decisions are conducted at the conceptual design phase. At this phase, it is more viable and less expensive to refine a design. PRA during conceptual design can help identify optimal areas for investments of further analysis.

More recently, Fragola & Putney [1] developed a "Lego-Block" approach for updating pre-existing shuttle developed PRA models and associated data sets to analyze new launcher functions. The "Lego-Block" model includes a functional decomposition of the shuttle, and the blocks represent the various functions. These blocks are reconstructed and extended to alternative vehicles by experienced experts within reasonable time and resource constraints.

The increasing significance of probabilistic risk assessment in the context of a TeamX like environment is reinforced by the appearance of new suggested approaches in the recent literature [2, 10, and 11].

2.2 *Risk Assessment in TeamX*

The process used routinely for risk assessment in the TeamX allows for the identification, assessment and synthesis of the risk items perceived during the design process. The risk chair is responsible for identifying the relevant risk items and communicating them to the relevant experts using a distributed software tool, RAP [5]. Each of the experts, in turn, assesses the risks sent to them, and adds any additional risks they perceive in their design. Engineers deliberate on the risk items, and come to a consensus about their relative significance during the sessions. The risks are then synthesized into an overall risk report after deliberations in the team.

3. EXPERIMENTS

3.1 Mars Aerocapture PRA

The objective of the study conducted in TeamX was to provide the customer the necessary information to enable them to build a probabilistic risk assessment model for aerocapture at Mars. This model would be used for comparing the risks of different types of Mars orbit insertion, namely, aerocapture, aerobraking, and propulsive capture. The team considered several previously designed missions for Mars Sample Return that used Aerobraking and propulsive as the means for orbit insertion, and made the necessary changes for an Aerocapture study. Throughout the design sessions, the team members expressed their expert opinions about the significant assumptions, and events, and the risk elements along with their severity and correlation to the events. Also, per the customer's request, the discipline experts provided schematics of their subsystem designs and responded to specific questions posed by the customers. In particular, the PRA team had identified several major risk elements for aerocapture that the team elaborated upon. These risk elements included:

•Navigational delivery errors/entry angle
•Aeroheating and thermal loads
•Thruster capability to react to aerodynamic demands used to control capture (ACS)
•GN&C
•Atmospheric variability at Mars
•Separation interface for aeroshell

Because the customer's objective was to build a Probabilistic Risk Assessment (PRA) model based on this design, the design team members made an extra effort to generate the information necessary for conducting the PRA. This information was mainly captured through RAP (Risk & Rationale Assessment Program), which is the tool used in TeamX for risk data collection, communication, and synthesis. This data was then used for building risk models with several different risk modeling tools. These tools included the Defect Detection & Prevention tool (DDP), the Galileo ASSAP dynamic fault tree solver, the Quantitative Risk Assessment System (QRAS). The models built with these tools each serve a different purpose. We initially built a system level model using DDP. Analyzing this model helped us identify the vulnerable parts of the system. QRAS models were built to demonstrate the possible scenarios and sequences of events that lead to them, and test possible mitigations. Later, we built dynamic fault trees for the vulnerable system modules to analyze them further.

The programs that were used throughout the course of the case study to create risk models were:

1. Risk & Rationale Assessment Program (RAP)
2. Defect & Detection Prevention (DDP)
3. Quantitative Risk Assessment System (QRAS)
4. Galileo Dynamic Fault Tree solution software (Galileo)

Each risk analysis program had a unique role in producing the PRA of the case study.

RAP is a tool used by the members of TeamX to collect and synthesis expert opinions on risk. The approach for collection and assessment of risk-related information is described in [5].

DDP is a tool [12, 13] used to build broad models of the system. This model structures the mission information in terms of an objective tree, a risk tree and a mitigation tree, and the numeric dependencies between the different elements of each of these trees.

QRAS is one of the main Probabilistic Risk Assessment (PRA) tools [6] on the market. This tool produces event trees and their correlation with risk elements in the system. The QRAS models provide a visual representation of the mission hierarchy.

Galileo dynamic fault tree solution software generates dynamic fault trees of the system architecture [15]. The Galileo models give us insight into the subtle dependencies within the system, and the vulnerable elements at both a quantitative and qualitative level. The dependencies within the system can be observed in the graphical representation of these fault trees. The reliability of the subsystem can be computed by allocating failure rates to each of the components and running the model.

Detailed information about this case study can be found in [13].

3.2 Mars Odyssey and Mars Telecomm Orbiter

The goal of the Mars Odyssey (MO) study in TeamX was to adopt the existing Mars Odyssey design in the subsystem templates and use some recently introduced modeling techniques within the team environment to experiment with refining the existing design. During the first week, the main task was to use all the available information about the Mars Odyssey project to build the related design into the TeamX spreadsheet. Independently from TeamX, we had built risk models for this project using the Galileo Dynamic Fault Tree analysis tool as part of a project for assessing the robustness of the Mars Relay Network. More information about this study will appear in [16]. It turns out that the team study was very effective in helping us update the pre-built risk models and refining them accordingly. More specifically, the team helped us better assess the criticality of the failure of various components or subsystems. In some occasions, they suggested possible work arounds that could prevent the system failure. This information made us realize that many of the failures will result in degraded states, but not mission failure. In addition, since our risk models are extremely sensitive to the expert opinions and the expert interpretation of the failure information, obtaining more expert opinions was useful for updating the risk information.

The Mars Telecom Orbiter (MTO) design was developed by TeamX and the study report was available to us. This study looked at multiple options for the propulsion system and the launch date as well. In addition, it included information about some of the unique features that were being considered for the orbiter. These features were an Orbiting Sample Capsule, and a Rendezvous and Autonomous Navigation experiment. The report also included a risk report which listed and ranked some of the major risk items identified during the study. We used this information, along with information obtained from the project Mission Assurance Manager to develop risk models for this orbiter.

4. LESSONS LEARNED

The experiments described in the previous section gave us a better understanding about the utility of probabilistic risk assessment in a TeamX like environment, and the utility of a

TeamX like environment for conducting PRA studies.

On one hand, it became clear that TeamX provides an optimal environment for the review and verification of existing risk models. Therefore, one of the utilities of TeamX is for risk "red team reviews". On the other hand, we realized that TeamX can be used for generating a creative list of events, assumptions and risks associated with a design that can be used for generating PRA models after the fact. Our underlying software tool, RAP allows for the identification of events and assumptions, and for linking the events with the risk items. The events identified by the team members were very creative and different from those typically included in PRA studies. Therefore we realized that involving the entire design team in determining the elements of a PRA study helps generate out of the box information. Since one of the main challenges in any PRA study is the determination of the events and the failure modes of the system elements in the presence of these events this can provide considerable benefit.

The different design sessions conducted in TeamX are classified based on the target body (e.g. Mars, Moon, and Earth Science) and the type of mission (e.g. Science, Technology). There is significant overlap in the functions the spacecraft needs to perform, and the main events it encounters during each class of mission. Therefore, it's possible to build high level reference PRA models for each class of mission, and update them during the timeframe of a study (which is usually a week) to include some risk information in the report.

Currently, in TeamX, many design decisions are made on the fly and optimized through verbal discussions and expert assessments by the individual designers. In order to be able to exercise any kind of risk model, even pre-existing ones, it' necessary to make changes to the design process to accommodate the extra time and effort it takes to run these models. This extra time and effort relates to collecting the necessary information from the team members , tweaking the pre-canned models to represent this information, running it to generate results, and finally discussing the results with the team so they consider it as input to their decision making process.

Another important piece of information is the data that is used for exercising the models. Our experiments demonstrate the sensitivity of our results to even the expert interpretation of the objective failure data. In order to get consistent results across the different studies, it's important to use consistent data sets. This is often a problem in TeamX, because the risk information is mainly generated from expert opinions and the experts are not necessarily the same for the different studies. This problem can be mitigated as we generate a larger library of risk information.

5. CONCLUSIONS & FUTURE DIRECTIONS

The main conclusions of this study can be summarized as follow:

1. In order to build PRA models in real time, it's necessary to start with a reference PRA for a similar type of mission and refine as you go along.
2. TeamX can be used for verifying existing risk models using designer expert opinions.
3. Design and risk information generated during the TeamX session can be used for building PRA models after the design session.

Following are some of our plans for further infusion of PRA in the TeamX environment:

1. Continue building reference PRA's for the different classes of missions studied in TeamX.
2. Experiment with these reference PRA's in the real time design sessions.
3. Utilize the TeamX environment for PRA red team reviews.
4. Utilize the TeamX environment for generating the design and risk information for building PRA models after the fact.

6. 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.

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.

7. REFERENCES

[1] J. Fragola & Bl. Putney, "A Risk Evaluation Approach for Safety in Aerospace Preliminary Design',

[2] H. McManus, D. Hastings, and J. Warmkessel, "New Methods for Rapid Architecture Selection and Conceptual Design", *Journal of Spacecraft and Rockets, Vol 41, No. 1, January-February 2004.*

[3] N. Smith and S. Mahadevan, "Probabilistic Methods for Aerospace System Conceptual Design" *Journal of Spacecraft and Rockets, Vol. 40, No. 3, May-June 2003*

[4] J. Chachere, J. Kunz, and R. Levitt, " Observation, Theory and Simulation of Integrated Concurrent Engineering: Risk Analysis Using Formal Models of Radicl Project Acceleration, *CIFE Working Paper # WP088, August 2004, Stanford University*

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

[6] Mark, G. (2002). Extreme collaboration. *Communications of the ACM. Vol. 45(6), pp.89-93*

[7] *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.

[8] Joanne Bechta Dugan, Salvatore Bavuso, and Mark Boyd. "Dynamic fault tree models for fault tolerant computer systems." In *IEEE Transactions on Reliability*, 41(3), September 1992, pp. 363 - 377.

[9] L. Meshkat, L. Xing, S. Donohue & Y. Ou An Overview of the Phase Modular Fault Tree Approach to Phased Mission System Analysis;; *Proceedings of the Space Mission Challenges for Information Technology (SMC-IT 2003)*, Pasadena, CA July 13-16 2003

[10] J.L. Benjamin, and M.E. Pate-Cornell, "Risk Chair for Concurrent Design Engineering: Satellite Swarm Illustration", *Journal of Spacecraft and Rockets, Vol. 41, No. 1, 2004, pp. 51-59.*

[11] A. Farhang Mehr & I. Tumer " A New Approach to Probabilistic Risk Analysis in Concurrent and Distributed Design of Aerospace Systems" *Proceeeings of IDETC/DAC, Sep. 24-26 2005, Long Beach, CA.*

[12] 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.

[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.

[14] Kevin J. Sullivan, Joanne Bechta Dugan and David Coppit, *"The Galileo Fault Tree Analysis Tool,"* Proceedings of the 29th International Conference on Fault-Tolerant Computing (FTCS-29), 1999.

[15] J. Scherbenski, L. Meshkat, "A Case Study for Risk Assessment & Modeling inConceptual Concurrent Design" JPL Technical Report.

[16] L. Meshkat, A. Girerd, C.Edwards, "An Integrated Approach for the Probabilistic Risk Assessment of the Mars Relay Network", to be published in the *Proceedings of the Reliability & Maintainability Symposium, January 2006*