Use of Probabilistic Risk Assessments for the International Space Station Program

Jeevan Perera
NASA-Johnson Space Center
Houston, Texas 77058
(281) 483-5814
jeevan.s.perera@nasa.gov

Jerry Holsomback
NASA-Johnson Space Center
Houston, Texas 77058
(281) 244-7956
jerry.b.holsomback@nasa.gov

Abstract—The purpose of risk management is to identify what can go wrong, how likely it is for these to occur, and what are the consequences if they were to occur. The International Space Station (ISS) Program office uses a continuous risk management process in identifying, analyzing, planning, tracking, controlling and communicating risks. This strategy manages risk by (i) embedding risk management processes into normal day-to-day activities to identify and help manage any risks or potential threats, (ii) facilitating risk-management processes and analyses by providing analytical support and tools.

One of the key quantitative risk analysis methods employed by the ISS program is the Probabilistic Risk Assessment (PRA) modeling techniques. PRA is a comprehensive, structured and logical analysis method for identifying and assessing risks in complex technological systems for the purpose of cost-effectively improving their safety and performance. The International Space Station has been modeled using this PRA methodology and is now used extensively by program management to make strategic decisions. The PRA results can be used as a powerful decision-making tool in support of design, operations, and prioritizing upgrade or reconfiguration decisions. The process helps identify potential new risks, analyze existing risks and subsequently can weigh different options available to the Program to mitigate those risks. The ISS PRA captures possible accident scenarios that lead to several undesired consequences called End States. Some background into the PRA methodology including examples of trade studies recently conducted for the ISS Program will be highlighted in this paper.

TABLE OF CONTENTS

1. INTRODUCTION	1
2. PRA METHODOLOGY	2

3. SAMPLE OF TRADE STUDIES UTILIZED BY PROGRAM MANAGEMENT	4
4. CONCLUSION	6
5. REFERENCES	6

1. INTRODUCTION

Probabilistic Risk Assessment (PRA) has, over the last several decades, evolved into a technical discipline capable of logically, systematically, and comprehensively assessing the weaknesses and vulnerabilities of complex systems and facilities that can adversely impact safety, productivity and mission success. Its usefulness has been tested in many industries including aerospace, electrical generation, petrochemical and defense. The most useful applications of PRA have been in complex systems subject to low-probability high-consequence (detrimental) scenarios or to complex scenarios consisting of chains of events that lead to adverse conditions or other impacts on the systems. Impacts may include those that appear to be slight or insignificant but collectively can interact to cause high severity consequences.

At NASA, the requirement for performing a quantitative risk assessment is contained in a NASA Policy Directive, (NASA Policy for Safety and Mission Success, NPD 8700.1). This policy directive states that the intent of the agency is to "maximize the likelihood of mission success by using qualitative or quantitative risk assessment techniques to identify and understand the risks, take appropriate steps to control or mitigate the risks, and then accept only reasonable and appropriate levels of residual risk before proceeding with a mission." It stresses that Project Management must consider the use of PRA in the development, testing and operations of the program/project. The policy mandates PRA for those programs/projects that involve scenarios, chains of events or activities, which could result in death or serious injury to the public, astronauts,

¹ U.S. Government work not protected by U.S. copyright

² IEEEAC paper #1007, Version 4, Updated 8 January 2004

pilots, or the NASA workforce, or the loss of high-value equipment and property.

NASA encourages its project managers to use PRA and associated analyses (e.g., uncertainty and sensitivity analyses, risk importance measures, etc.) to support management decisions to improve safety and performance throughout all life cycle phases. These analyses are used to identify and analyze new, existing or changing hazards introduced with each evolving phase of a project. In addition, the project/mission design or operating and implementation plans are updated to reflect insights from PRA analysis. These insights are also used to reinforce or modify existing relevant management decisions or even to generate new management decisions.

The Space Station Program uses Probabilistic Risk Assessment (PRA) to assess factors contributing to risk and to determine their relative impacts within ISS development and operations. Due to the staged nature of the Station's assembly sequence (construction of the Station alone will span many years and many Shuttle and Russian launch vehicle flights), the PRA is being developed in a phased approach. The ISS PRA model can currently assess the Station risk at assembly sequence stages 5A, 7A, 12A.1, and ULF2. The 1E, 1J and assembly complete stages are currently being developed to assist in future strategic decisions. Intermediate configurations that need to be analyzed can be easily obtained by adjusting one of these key configurations.

2. PRA METHODOLOGY

Before a sampling of the recent trade studies developed for the ISS program management is presented, PRA background and its methodology will be briefly discussed.

A PRA models a set of scenarios, their frequencies and the associated consequences. The effort required to perform this modeling is justified since it can help in optimizing a design by factoring in safety considerations, or during operational phases, reveal the safest procedures for workarounds or complying with operational constraints.

Modeling a scenario under PRA begins by considering any initiating events that eventually could damage the Station or harm its inhabitants. Under this modeling scheme, each initiating event can result in one or more pivotal events that terminate in one or more predefined End States (see Figure 1). The logic process starting with an initiator followed by many conditional events (pivotal events), finally ending with one or more End States, is referred to as an Event Sequence Diagram (ESD). These ESDs are derived from flight rules, hazard reports, Failure Modes and Effects Analysis (FMEA), evaluation of Critical Item List (CIL), operations guidelines and system engineering knowledge.

Figure 1 – Elements of a PRA Model

In addition, this risk assessment technique models the logical inter-relationships, dependencies, and reliability of the system. It is important that the uncertainties in the natural variability of physical processes (i.e., aleatory uncertainty) and the uncertainties in knowledge of these processes (i.e., epistemic uncertainty) are included in the model to convey the uncertainty of the results. Data uncertainty is an integral component of the model.

Figure 2 conceptually illustrates how the PRA model is developed by a variety of these logical constructions discussed above. The PRA model is developed by systematically decomposing the ISS to reveal which systems and functions must work at what levels to meet the different Space Station requirements. The Master Logic Diagram (MLD) provides a systematic framework to perform this decomposition. The MLD helps to identify the initiators that could prevent the Station from maintaining habitability or satisfying other functional requirements. As mentioned previously, these initiator events are the beginning of the analysis depicted in the Event Sequence Diagrams (ESDs).

Figure 2 – ISS PRA Model Construction

Initiating Event

The initiating event is an event which perturbs the modeled system requiring human intervention (from operators or crew-members) and/or system responses. Depending on what occurs subsequently (system and/or human response), the system will either go back to a "normal" operating state or progress to a "bad" state (see discussion of End States to follow). These responses can be classified as either:

- Protective – an event that reduces the likelihood the initiating event will produce an undesired end state,
- Mitigative – an event that reduces the severity of the end state,
- Aggravative – an event that increases the severity of the end state, the frequency of reaching an undesired end state, or both, or
- Benign – an event that has little or no effect on the course of the scenario although it may have been perceived as a contributor prior to the analysis.

Pivotal Events & Fault Trees

Pivotal events capture the resulting system responses after an initiating event. Pivotal events are those events that must occur in order to prevent the initiating event from propagating further. These may take the form of systems responses whether hardware or software, procedural steps including crew or ground intervention, physical conditions, or time constraints. The success or failure of the system and/or human responses (discussed above), or possibly the occurrence or non-occurrence of some external conditions or key phenomena will determine the result of a pivotal event.

The probabilities or outcomes of the pivotal events are usually determined by the development of fault trees. In other words, fault trees are used to determine the probability of the two paths (success or failure) of the pivotal event. Fault trees are logical, structured mechanisms that can help identify potential causes of system failure. They graphically represent the interaction of failures and other events in the system by representing the system's architecture and operation. Major fault trees for US and Russian segments of the Space Station were developed in the areas of:

- Electrical power and distribution
- Thermal control
- Command & data handling
- Attitude control
- Propulsion
- Communication & tracking
- Guidance, navigation and control
- Life support systems

These fault trees model interdependencies among the distributed systems by including the interactions with all supporting equipment. The fault trees for the ISS PRA were developed from many sources including training manuals, systems handbooks, architecture description documents and detailed technical drawings and schematics.

The bottom levels of the fault trees are the basic events of the model (lowest level that is modeled). The data to support these fault trees are based on failure histories and other historical data sources.

End States

The results of the PRA are calculated by combining all like End States across all the ESDs. Resultantly, the mean and distribution of the probability of occurrence of each of the End State can be calculated.

The ISS Program goals for the study and analysis capability were to examine those scenarios that can lead to:

- Loss of the Station (whether sudden catastrophic or through progressive loss of critical systems)
- Loss of a crewmember
- Situations requiring evacuation.

These are considered the critical End States and are the key measure in many trade analyses done for the program.

The non-critical End States that were added to the modeling were:

- Loss of a system (critical system failure, even though there is not loss of station)
- Loss of a module (where an ISS module is no longer inhabitable or operational)
- Collision (visiting vehicle collides with the Station).

All these conditions above (3 critical and 3 non-critical) are the six End States that the ISS PRA model utilizes.

Figure 3 show an example of an event sequence diagram starting with an initiator (shown as a green circle) progressing through several pivotal events (shown as a decision boxes) and leading to several potential outcomes (End States shown as diamonds).

Figure 3 – Event Sequence Diagram Example

3. SAMPLE OF TRADE STUDIES UTILIZED BY PROGRAM MANAGEMENT

Several recent trade studies will be highlighted in this section to demonstrate the wide variety of analysis that the ISS PRA provides.

SM Window Cover vs Vozdukh Spare

As the team completed the first phase of the model development, the Program Manager asked if the PRA could be used to quantify the risks with an immediate manifest decision. There had been ongoing issues with the carbon-dioxide removal systems on-board the Station. Parts of the Russian system (Vozdukh) had failed and been repaired. Shortly after the launch of the US Lab Module, the US Carbon Dioxide Removal Assembly (CDRA) also failed. The program was looking to fly spare parts for the Vozdukh system on the next shuttle flight. The issue was, in order to fly these parts something already manifested would have to be removed. The item under consideration was a window cover for the Service Module designed to protect against orbital debris strikes. The question posed was; which item provides the most risk reduction?

The results showed that providing Vozdukh with spare parts would improve risk by an order of magnitude while the window cover improved risk by a small margin. This result confirmed the "gut feel" the Program Manager had based on all the other input he had received. This study allowed him the ability to quantitatively measure the impact of his decision. The next Shuttle flight was remanifested and the spare parts suggested were flown.

Figure 4 – Event Sequence Diagram Example

Sensitivity Analysis: DDCU Quantification

During the integration and test of the DC-to-DC Converter Units (DDCU) used in the US Segment, NASA Independent Assessment (IA) review teams indicated that the reliability of the DDCU's would be less than advertised. The discrepancy in mean time between failures (MTBFs) was several orders of magnitude, IA predicting an MTBF of 3,440 hours, the logistics and maintenance team using

800,000 hours and the program requirement of 87,600 hours. The program requested that the PRA be used to determine whether this discrepancy was significant from a system perspective. A baseline value was calculated from a synthesis of industry data -- 34,000 hours.

The results showed that even though there is redundancy in the system, the early phase of the assembly was vulnerable to DDCU failures. The study revealed that should the DDCU be as bad as predicted by the independent assessment organization, the impact to the Station operations would be substantial since there would be an order of magnitude increase in risk. However, if the actual MTBF were closer to the ISS requirement or the logistics & maintenance team's prediction, the risk would be only marginally better than the baseline estimate.

Figure 5 – Event Sequence Diagram Example

Postponing Maintenance Activities

Some studies performed for program had indicated that the Station would require significant crew hours to maintain an operating and functioning Station. These increased maintenance activities (more than originally anticipated) would result in only about 4 hours of science conducted every day. Since reducing maintenance activities would free up the crew to conduct science, a trade study was performed to assess if there would be more science, if the program deferred all maintenance activities to times when the Space Shuttle was docked to the Station. During routine Shuttle dockings, Shuttle crewmembers could be trained and then dedicated to make the needed repairs and to perform all preventative maintenance. However, the results as seen in Figure 6 show that the science time achieved by adopting this plan would actually decrease. While in the short term, the number of hours would increase because more crew members can perform science, the deferred maintenance activities would increase the probability of reaching a catastrophic end state like evacuation. Therefore, in the long term, there would be a greater probability of being unmanned due to evacuation or greater amount of time spent

performing critical maintenance (due to preventative maintenance being deferred). Resultantly, less science will actually be performed in the long run. The next step in the analysis was to temper this affect by deferring all but the more critical maintenance to dedicated Shuttle maintenance crews. This result showed that there was a possible improvement of 2 to 3 times the amount of science compared to retaining the baseline maintenance plans.

Figure 6 – Event Sequence Diagram Example

CRV-Soyuz Comparison

To provide a more robust and medically safe escape system for the crew, the program always considered either replacing or complementing the Soyuz vehicle (as the escape system). At the time, the X-38 program (a US crew return vehicle) was in development. A PRA trade study was performed to determine the best escape vehicle configuration for varying crew sizes. The analysis revealed that the capability to return several types of medical cases was the key driver. For instance, the Soyuz vehicle cannot transport crewmembers needing an IV or when an injured crewmember must be transported in a prone position. Due to this fact, the X-38 rescue vehicle with the expanded medical capabilities improved risk more than two redundant Soyuz vehicles (see Figure 7). However, the enhanced redundancy achieved by two independently designed and built system (X-38 and Soyuz) in complement would achieved the best risk reduction.

Figure 7 – Event Sequence Diagram Example

Uncrewed and Tended Station Trade Study

One of the more useful applications of the PRA came in the aftermath of the Columbia tragedy in February 2003. The program manager was faced with examining the prospect of maintaining a crew on orbit without the Shuttle (which had provided the main logistical support and crew exchanges for the Station). Logistics and provisioning studies had indicated that water and food shortages might force the program to reduce the crew size from 3 to 2. Furthermore, these logistics constraints (not having the Shuttle which provides the main resupply capability for the Station) could even force the Station to be unmanned for temporary periods. The Program Manager wanted to know the relative risks of losing the station with 3 crewmembers, 2 crewmembers or leaving the station unmanned. Was there any added risk incurred by reducing the crew size, or even more drastic, by unmanning the Station? A trade study was performed to compare these options by analyzing the scenarios for 6 months and one-year evaluation periods. The results, as seen on Figure 8, show that there is almost a magnitude increase in the loss of Station probabilities by having crewmembers on board versus unmanning the Station. Unmanning the Station leaves it vulnerable to failures, which cannot be repaired since no crew would be on-board. History had validated this conclusion, since the crew had been able to repair critical problems over the first several years of the Station's life.

Figure 8 – Loss of Station Probabilities Comparing Different Crew Sizes

The main drivers that led to loss of Station in this analysis (in either the manned or unmanned cases) were the failure of both internal or both external temperature control system (TCS) loops, which leads to the complete loss of US TCS. Another significant driver was destruction/severe damage to the Station due to MMOD penetration. In the unmanned case, additional drivers are present due to the unavailability of crew to address critical failures or problems. These drivers include the failure of all three Command and Control computers which would cause a loss of control for all

station functions, failure of the Russian Control Module's TCS, multiple failures within the communication & tracking system cause the complete loss of the communication & tracking function, and the complete failure of US power generation

The main critical systems that were vulnerable to loss as shown in Figure 9 were failure of both internal or both external TCS loops. Another driver for system loss was the failure of the propulsion system that would result in the loss of propulsive attitude control (common cause failure of all positive or negative roll thrusters) for the Station. All of these systems that drive the loss of system probabilities are, as expected, worse for the un-manned case as the manned cases.

Figure 9 – Loss of Major System Probabilities Comparing Different Crew Sizes

This study also proved that the model was flexible enough to rapidly reconfigure for the current conditions and environment of the station, apply the various new constraints based on the needs of the program and produce pertinent and useful results within days.

4. CONCLUSION

Probabilistic Risk Assessment (PRA) is a multi-disciplinary method used to assess many factors and to determine their relative significance within a system. The PRA models are used to assess, manage, and, if necessary, quantitatively justify the need to reduce the risk of any options being considered by management (whether in design, test, operation, disposal, etc.).

The ISS PRA is scenario-based model that has been developed over the last several years and models specific configurations of the Space Station. The reliability data driving the model has been statistically updated in a traceable manner. These include hardware failures, software errors, human error, common cause failures, and

external events. The rates are updated as the Program obtains relevant failures/errors from operational use of the Station.

The program has relied on the analysis that the PRA model provides for many varied programmatic decisions. The ISS PRA results are used as a powerful decision-making tool in support of design, operations, and upgrade alternative decisions.

The PRA can develop a trade study to show ISS program management the effect of two or more options (design, operations or upgrade) and the magnitude of the resultant change on safety risk to the Station. Although the model can derive probabilities of any given End State, its real value is in comparative analysis (due to the large uncertainties in the results). The ISS PRA model continues to be enhanced, as new trade studies are demanded.

5. REFERENCES

- [1] E.E. Lewis, *Introduction to Reliability Engineering*, New York, John Wiley & Sons, 1987 .
- [2] "NASA Policy for Safety and Mission Success," NASA Policy Directive 8700.1, NASA, Washington, DC.
- [3] "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners," 2002 *Office of Safety and Mission Assurance*; NASA, Washington, DC.
- [4] "Probabilistic Risk Assessment of the International Space Station Phase II – Stage 7A Configuration," ISSPRA-00-40, 2002, *International Space Station Program Office*, NASA, Houston.

BIOGRAPHY

Jeevan Perera's work involves leading a risk management team implementing tools and process for manned space programs including the International Space Station, the Space Shuttle and the Orbital Space Plane. In this capacity, he oversees both quantitative and qualitative risk analysis processes. Dr. Perera has designed, developed, implemented and improved the International Space Station risk management process using a phased approach including providing the necessary supporting tools, applications and corresponding training. In addition, Dr. Perera has overseen risk management assessments of ISS Program systems and procedures through Probabilistic Risk Assessments (PRA) and other quantitative methods for strategic & logistics planning and real-time operational support. He has a bachelor's degree in Aerospace Engineering, a master's degree in Industrial Engineering, a Doctorate in Jurisprudence, and a Doctorate in Industrial Engineering.