Applications of the International Space Station Probabilistic Risk Assessment Model

Recently the International Space Station (ISS) has incorporated more Probabilistic Risk Assessments (PRAs) in the decision making process for significant issues. Future PRAs will have major impact to ISS and future spacecraft development and operations. These PRAs will have their foundation in the current complete ISS PRA model and the current PRA trade studies that are being analyzed as requested by ISS Program stakeholders. ISS PRAs have recently helped in the decision making process for determining reliability requirements for future NASA spacecraft and commercial spacecraft, making crew rescue decisions, as well as making operational requirements for ISS orbital orientation, planning Extravehicular activities (EVAs) and robotic operations. This paper will describe some applications of the ISS PRA model and how they impacted the final decision. This paper will discuss future analysis topics such as life extension, requirements of new commercial vehicles visiting ISS.

APPLICATIONS OF THE INTERNATIONAL SPACE STATION PROBABILISTIC RISK ASSESSMENT MODEL

Warren Grant[(1)], Michael Lutomski[(2)]

[(1)]ARES Corporation, 1440 Chapin Ave, Ste. 390 Burlingame, CA 94010, USA , Email:wgrant@arescorporation.com
[(2)]NASA,,2101 NASA Parkway, Houston, TX 77058 USA, Email:michael.g.lutomski@nasa.gov

ABSTRACT

The International Space Station (ISS) program is continuing to expand the use of Probabilistic Risk Assessments (PRAs). The use of PRAs in the ISS decision making process has proven very successful over the past 8 years. PRAs are used in the decision making process to address significant operational and design issues as well as to identify, communicate, and mitigate risks. Future PRAs are expected to have major impacts on not only the ISS, but also future NASA programs and projects. Many of these PRAs will have their foundation in the current ISS PRA model and in PRA trade studies that are being developed for the ISS Program. ISS PRAs have supported:

- Development of reliability requirements for future NASA and commercial spacecraft,
- Determination of inherent risk for visiting vehicles,
- Evaluation of potential crew rescue scenarios,
- Operational requirements and alternatives,
- Planning of Extravehicular activities (EVAs) and,
- Evaluation of robotics operations.

This paper will describe some applications of the ISS PRA model and how they impacted the final decisions that were made.

1. INTRODUCTION

The ISS has been continuously manned for almost eleven years, longer than any other space station before. Now that its assembly has been completed, it is also the largest object to ever be built and operated in Earth orbit. Fifteen nations have been involved with its design, construction, and onboard research activities.

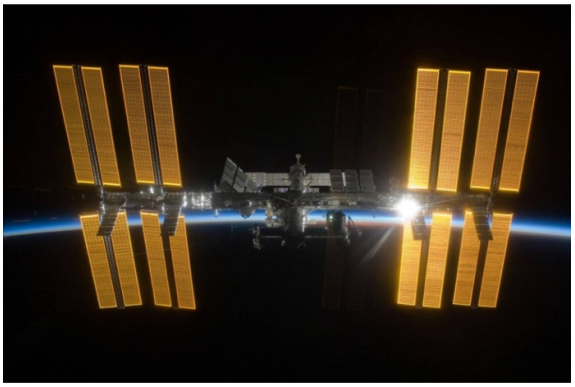

Figure 1, ISS Assembly Completed in Earth Orbit

Unlike the representations of manned spacecraft in science fiction, the ISS is an extremely complex vehicle that requires constant vigilance, attention to detail, and diligent evaluation of risk in order to preserve its mission and provide the safest possible environment for its crew.

In addition to various methods for identifying and qualifying the many and varied risks associated with day-to-day operation of the ISS, PRA provides a quantitative means of risk analysis to support program level discussions. An understanding of risk and its implications can be of significant value as decisions are made for a large number of issues related to the design and operation of the ISS.

2. A PRIMER FOR PRA

First, it is useful to understand what a risk is. A Risk is any future event with a negative consequence that has some probability of occurring. It is a combination of the likelihood of occurrence and the severity of the consequence. It usually represents an issue whose resolution is unlikely without focused management effort. *An ISS Program risk poses a threat to the crew or vehicle safety, program cost, schedule, or major mission objective*.

Types of risk include cost, schedule, and technical risk. Technical risks may impact mission success, operational performance, and/or safety. When assessing risk, questions such as what can go wrong, how likely is it, and what is the consequence if the risk is realized, are evaluated.

PRAs, as applied in the ISS Program, specifically address technical risk and attempt to quantify the likelihood of a risk or answer the question "how likely is it."

Given thousands of space stations operating for dozens of years, common statistics could be used to determine reasonably accurate predictions for failure. However we have only one space station and it has had minimal experience and no catastrophic failures. Therefore there will rarely be any statistically significant data available. PRAs can provide a quantitative measure of risk for rare events.

The ISS PRA model provides probabilities for a select number of critical end states. The end states of concern are defined by the ISS Program or the organization requesting the analysis. A set of scenarios representing a sequence of failures and their frequencies were developed. Logical analysis was then applied to calculate the probability of occurrence for each scenario. Initiating events are modelled with other conditional events that eventually terminate with the realization of an end state via the given scenario. In the ISS PRA model, failures propagate through fault tress up to event trees which represent a scenario or event sequence.

To create a PRA model, a detailed review of systems, components, hazard reports, and technical documents is performed. Scenarios in the form of event sequence diagrams and event trees are developed to be representative of systems functionality and ISS flight operations. The end states provide a quantitative value for the probability of failure including the uncertainty associated with that value. Specific failures that contribute to the end states are also important to understand, since it allows decision makers to not only mitigate the risk, but also to effectively evaluate alternatives.

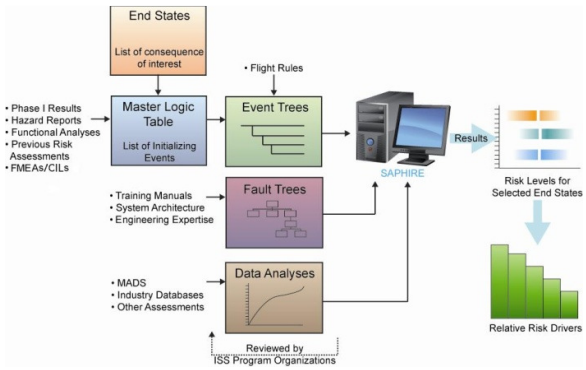

Figure 2, PRA Process

3. UTILIZATION OF ISS PRA

The objectives of PRA are to:

- Identify & evaluate risks to program/project goals and communicate them to management,
- Support risk informed decision making with quantifiable data, and
- Synchronize with other program/project process and activities in engineering, S&MA, Operations.

The products provided from PRA analyses are risk models; probability distribution functions for end states, events, and accident scenarios; and operational trades and sensitivity analyses.

There are generally two types of analyses that are performed using PRA. The first utilizes the complete ISS PRA model to evaluate end states and their contributors. Different time periods, selected scenarios, and a limited number of "what if" scenarios can be performed with this model.

The second is the focused PRA analysis. This often utilizes a part of the ISS PRA model and adds additional detail or modifies a scenario. Unique models are also developed for these analyses when warranted.

4. THE ISS PRA MODEL

The ISS PRA model is highly detailed and complex. NASA requirements documents mandate its development, but do not specifically prescribe the extent of its use. In the ISS program, PRA has gained increased acceptance since the common use of it began in 2000.

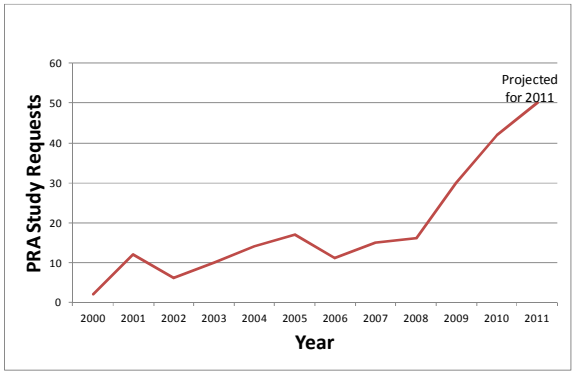

Figure 3, PRA Requests are Increasing

Effective communication, quick turnaround times, and the demonstrated applicability of PRA have contributed to its increased use and value to the program. The ISS PRA model and focused PRA studies are now used to provide additional information to stakeholders representing nearly every aspect of the program.

4.1. ISS PRA End States

The ISS PRA model focuses on providing a quantitative probability, including uncertainty bounds, for reaching three critical end states - Evacuation (EVAC), Loss of Crew (LOC), and Loss of Crew and Vehicle (LOCV). EVAC scenarios are those that are not immediately catastrophic but pose a threat to the crew, and would result in crew evacuation. The LOC end state includes scenarios that result in the death of one or more crewmembers. It is restricted to those cases where death is immediate or evacuation is not possible.

LOCV includes scenarios that result in the immediate loss of the ISS and crew. The crew would have insufficient time to take corrective action or evacuate.

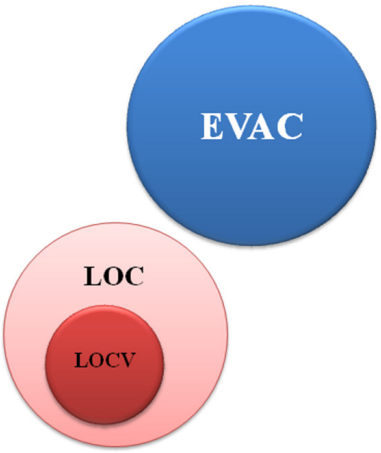

Figure 4, End State Relationships

The EVAC and LOC end states include all scenarios where one *or more* crew members are affected. This is important to communicate since one might initially believe that the EVAC end state means that the ISS is left with zero crew aboard. There are scenarios when an evacuation of three crew members occurs, but the other three crew members remain aboard.

4.2. PRA Model Scope

The PRA model for the ISS reflects the current configuration of the vehicle currently in orbit. Modules, systems, propulsive maneuvers, robotics and Extra-Vehicular Activities (EVA) are modelled. Phenomenological events such as fire and Micro-Meteoroid and Orbital Debris (MM-OD) are also analyzed. Results are provided for medical scenarios via an independent Integrated Medical Model (IMM) developed by experts in the medical field. The results of the IMM are incorporated into the ISS PRA so that those risks can be assessed with other PRA risks as modelled.

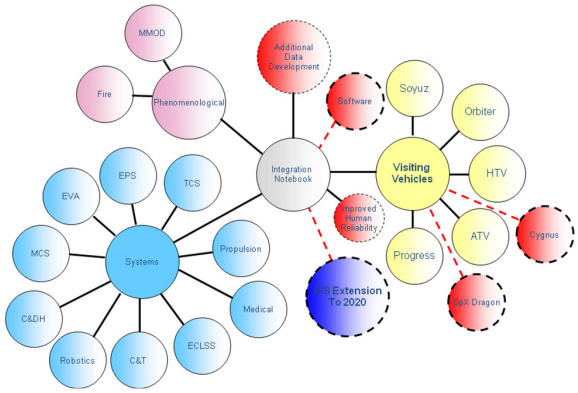

Figure 5, ISS PRA Model Scope

Repair events, uncertainty, and, where applicable, human reliability are also accounted for.

There are some things that are not modelled such as heroic actions. There is no reliable way to predict what actions might be taken that are outside of approved and trained flight rules and procedures. Software reliability had previously not been accounted for in the PRA model, but an effort is currently underway to provide a methodology to represent the risk associated with software.

Results are provided to program stakeholders in the form of description, scope, assumptions or initial conditions, numerical results with uncertainty, contributors, and written analysis. The analysis provides context and explanation of the results within the given set of assumptions. This will become more evident in the following section as specific studies are discussed.

5. SPECIFIC PRA STUDIES

Focussed PRA studies developed for specific scenarios comprise the majority of PRA work that is completed for the ISS program each year. Many of these studies begin with the ISS PRA model and are then customized with additional detail and analysis. There are also a large number that are developed independently. Many scenarios that are requested for analysis begin outside of the ISS PRA model scope. When a study provides additional information or reveals improvement opportunities for the ISS PRA model, it is incorporated in the next scheduled model update.

These studies provide an additional “data point” that, when evaluated with other information, contribute to decisions made for daily and future operations of the ISS. The following sections give specific examples of how the PRA methodology is employed in the ISS Program.

5.1. Mobile Transporter Trailing Umbilical System Risk from MM-OD Impacts

The Mobile Transporter (MT) is part of the Mobile Servicing System (MSS) on the ISS. It moves, or transports, the robotic arm, Canadarm 2. It runs along a rail on the outside of the ISS and was used extensively during ISS construction. It is still used for repairs and during some visiting vehicle operations.

The rail that the MT moves on allows it to transverse the entire length of the station. Along the length of the rail there are designated stopping points called work stations. The MT is powered by a Trailing Umbilical System (TUS) cable that is attached by a reel. As the MT moves between work stations the TUS cable is pulled out from the reel or retracted back in. When positioned at work station #4, the TUS cable is almost fully retracted and protected from MM-OD damage by the TUS reel housing.

Since the MT is an important operational asset, it is important to ensure its continued function by mitigating risk factors to the largest extent practical. A common practice was to minimize translations of the MT to preserve its operating life. After each operation the MT was left at its last worksite in lieu of the adding the additional operating time to return it to another worksite.

Figure 6, Mobile Transporter with Canadarm-2 and SPDM

The program concerns were as follows:

- If the MT is left parked for long periods of time at worksites other than worksite 4 at the center of the S0 truss, the TUS reel cables will be exposed to risk of MM-OD penetration over long periods of time
- Additional MT movement to park it at worksite #4 may result in decreased MM-OD risk to the TUS cables.
- Additional MT movement to park it at worksite #4 may result in increased risk of MT failure due to the increased operating time.

The PRA team was asked to quantify the probability of failure to compare these scenarios. The results of the analysis demonstrated close to two orders of magnitude difference in risk. It showed that damage to the MT was more likely to be from an MM-OD strike than from a hardware failure.

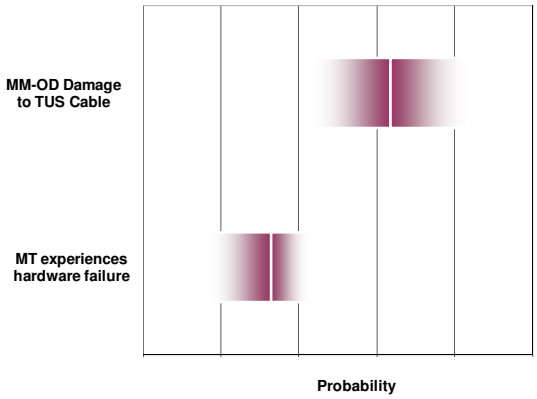

Figure 7, MT Risk Comparison

Using these results with other information, the program changed the practice of leaving the MT at its last worksite location. The MT is now returned to worksite #4 after each operation.

5.2. Drag-thru Risk for Temporary Crew Quarters

In 2009 a temporary crew quarters (CQ) was scheduled to be placed in the Japanese Experimental Module (JEM). Since this was to be a temporary location, a drag-thru cable was proposed that would provide caution and warning capability. The drag-thru in this case is a signal cable that is placed through the hatch way into the JEM. MM-OD penetrations represent a depression risk for the ISS and can be mitigated by closing hatches to isolate modules. A drag-thru would need to be removed in the event that the JEM hatch would need to be closed in an emergency.

The caution and warning capability in a CQ is of primary concern since it will alert the crew member if airflow is lost. A loss of air flow would allow a build up of carbon dioxide that would displace the amount oxygen for the crew member to breath. If sleeping, the crew member may notice this condition. Any one of two fans on the CQ would prevent this from occurring.

Figure 8, Crew Quarters

A PRA study was performed to compare the probability of losing airflow in the CQ to the risk of need to close the hatch in an emergency such fire or depress.

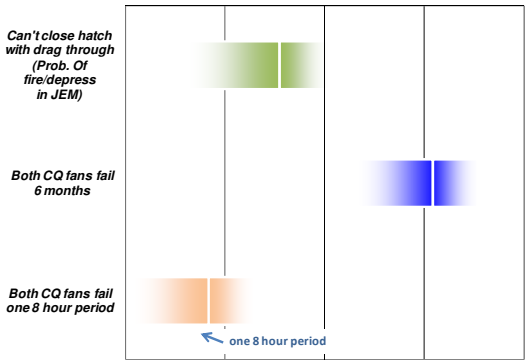

Figure 9, Drag-thru risk for JEM Temporary CQ

The study demonstrated that over a 6 month period (the average time for a crew increment) not having a caution and warning alarm capability in the CQ posed a greater risk. The probability of an emergency that require the JEM hatch to be closed was less.

The drag-thru was allowed for this temporary condition until the CQ was moved to its permanent location.

5.3. HTV Control Panel Failure Comparison to Portable Computer System with Backup

The use of drag-thru cables for power and data is a concern for the program. Drag-thrus run through hatches between modules and must be removed in the event of an emergency that requires the hatch to be closed. When an operation dictates the use of a drag-thru, each case must be evaluated independently and the risk assessed in order to keep their number to a minimum.

The H-II Transfer Vehicle (HTV) is a resupply vehicle designed by the Japan Aerospace Exploration Agency (JAXA). Once it autonomously approaches the ISS, the Canadarm-2 is used to "grapple" the vehicle so that it can be manually berthed to ISS. There is a critical time period during this operation where the ISS crew must watch for problems and respond to them quickly. The crew response to a failure is to issue an abort command to the HTV causing it to move away from the ISS.

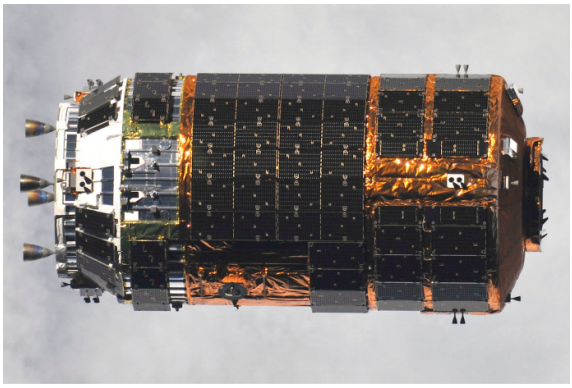

Figure 10, H-II Transfer Vehicle

When warranted, the abort command is sent via an HTV Control Panel (HCP). The HCP is stored in the JEM, but when in use, it is moved to the Cupola module.

Figure 11, HTV Control Panel (HCP)

The HCP must be connected to a panel in the JEM. This is accomplished using a drag-thru that must traverse through several modules before reaching the Cupola.
An alternative to the HCP exists that allows portable computer systems (PCS), much like a laptop computer, with special software to be used. Unlike the HCP,

however, PCSs are not specifically designed for the purpose of HTV rendezvous and were not subject to the same rigor for design and manufacture. The PCSs do not require a drag-thru.

A PRA was requested to quantitatively show the risk comparison between using the HCP and a PCS with a second PCS as a backup.

In this case the HCP was shown to be more reliable, however, there is only a small window of time when failure to send an abort command would be critical. When the probability of a required abort is coupled with the hardware failure probabilities of the HCP and PCSs, the overall probability for failure during an HTV rendezvous is very small for both scenarios. This led to a decision to use the PCSs for future missions after some additional analysis of the PCS software and command delay times.

5.4. Risk of Shock During Extravehicular Activity (EVA)

The ISS operates in an electrically conductive plasma environment. Both negative and positive potentials exist, but negative potentials are mitigated by plasma contactor units (PCU) that provide for ISS ground to plasma.

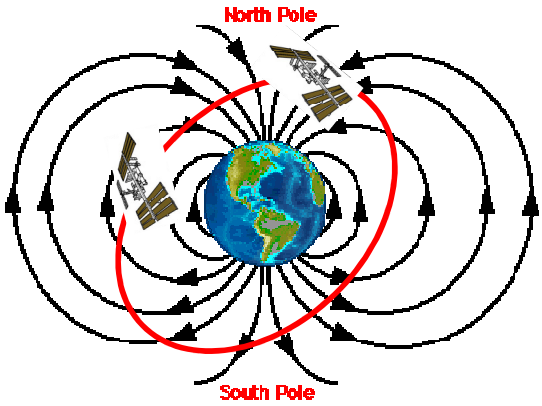

Figure 12, Magnetically Induced Voltages on the ISS

Positive charging is caused by magnetic induction as ISS passes through Earth's magnetic field lines at higher latitudes. The hazard must be mitigated when the EVA crew member will be working at the outside extremes of the ISS past the Solar Array Alpha Joints (SARJ). In these conditions the EVA crew is exposed to a shock hazard if a path through the crewman's body exists between the positively-charged ISS structure and negatively-charged plasma.

In order for this to occur, several events must occur simultaneously: ISS structure must be at a positive potential. A conductive part of the Extravehicular Mobility Unit (EMU) must contact a conductive part of the ISS. The crewman must be touching the inside of that conductive EMU part with either bare skin or by compressing a moist Liquid Cooling and Ventilation Garment (LCVG) against it. At the same time, the crewman must be touching the inside of either the Waist Bearing (WB) or the Body Seal Closure (BSC) while that part of the EMU is in contact with plasma.

Figure 13, Location of Potentially Exposed Surfaces on EMU

In order to understand the shock risk to the crew member, a PRA was performed using inputs from a team of experts from operations, safety, engineering, space medicine, environments and the EMU manufacturer. The analysis was performed for a 6.5 hour period during which the crew member would be exposed to the hazard.

For the purpose of this PRA, the model did not assess the severity of the shock, only the probability of its occurrence. These results were compared to the risk of a nominal EVA for perspective.

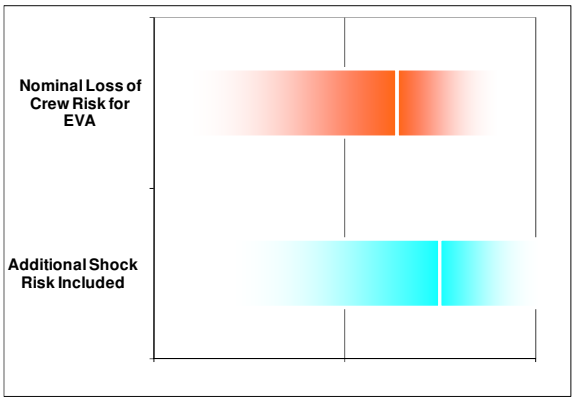

Figure 14, Nominal EVA Risk vs. Additional Positive Potential Shock Risk

This study supported a Non-conformance Report required to assess and approve the additional risk from potential shock hazards during a specific EVA. The PRA assisted in the identification of high likelihood areas on the EMU for a current path to the crew member. This information was then used to mitigate the high risk paths to make the EVA safer for the crew member.

6. CONCLUSION

PRA is being used more and more frequently as the ISS Program evolves. PRA is being used to support decisions with a wider range of risk scenarios and operational decisions in the ISS Program. The use of PRA has proven to be very valuable in the decision making process. The use of PRA has increased drastically since 2008. Effective means of communication with management and a willingness to work with a every Program organization has been key in fostering this trend.

Though it is not practical or recommended to utilize the results of a PRA alone, it has proven to be a valuable asset for a large number of design and operational decisions. Costs, schedule, experience, engineering judgement are still valuable and key factors in decision making. PRA has, and will continue, to provide logical analyses of risk that help ensure the safety and longevity of the only human space platform in existence today.