International Journal of Performability Engineering, Vol. 9, No. 6, November 2013, pp. 587-598.

Two Case Studies Illustrating the Management of Risks for the International Space Station

K. CARTER-JOURNET[1], J. CALHOUN[2], M. RAFTERY[3] and M. LUTOMSKI[4]

[1]*Senior Engineer/Scientist, ARES Technical Services, Houston, Texas 77058*
[2]*Junior Engineer/Scientist, ARES Technical Services, Houston, Texas 77058*
[3]*Risk Integrator, ARES Technical Services, Houston, Texas 77058*
[4]*Risk Manager, National Aeronautics and Space Administration, Houston, Texas, 77058*

(Received on March 20, 2013, revised on April 16 and May 01, 2013)

Abstract: The International Space Station (ISS) has been operating in space for over 14 years and permanently crewed for over 12 years. Throughout this time, the ISS Program has implemented and continually improved its risk management process. This ISS risk management process identifies risks that may exist and alternatives for mitigation if the risks are significant. Risk management has provided input that has been essential to the program management decision making process. Risks can be reduced, mitigated or accepted and are prioritized to ensure program resources are used as efficiently as possible. The ISS risk management process has increased the probability of success of the ISS mission objectives and overall crew safety.

This paper presents two case studies on how the ISS risk management process has been used to address specific areas of risk. The first case describes how the ISS Program has analyzed and mitigated the risk of Micrometeoroid Orbital Debris (MMOD) strikes to pressurized modules. MMOD has been a major safety concern since the beginning of the program. The second case study describes the risk assessment of Visiting Vehicle (VV) collisions. There has been a significant increase in the number of visiting vehicle flights to the ISS since the retirement of the Space Shuttle Program. This has caused an elevated cumulative risk of collision when considering the frequency of vehicle traffic to the ISS.

Keywords: *International Space Station, risk management, micrometeoroid orbital debris, visiting vehicle collisions, case studies*

1 Introduction

Risk management must be an active process. "*Governments are endeavoring to manage not only the interdependencies and interactions among hazards, between various systems and the forces influencing the overall context of risk management, but also the increasingly important international dimension of risk* (1)." This statement referenced the nuclear industry, but it is also appropriate to the International Space Station (ISS) since it is an international partnership (Canada, Japan, Russia, and the member countries of the European Space Agency) between 15 countries. A scientific project of this magnitude can yield rewards, but also introduces many risks. As a result, the ISS Program must be diligent in how it identifies, analyzes, and mitigates risk. This is accomplished by having a comprehensive plan in place that defines the purpose, approaches, roles and responsibilities, processes, and tools used to manage risks across the ISS Program and all of its partners (2).

Risk is evaluated in terms of likelihood and consequence. The consequences can be technical, safety, cost, or schedule related and a risk may possess a combination of these types of consequences. In the mature state and utilization phase of the ISS Program, today schedule and cost threats have become the program's top risks. Uncertainty analysis is an inherent part of the risk characterization. ISS program policy requires that action be taken

*Corresponding author's email: jessica.a.calhoun@nasa.gov to change designs, processes, or plans to mitigate the impact that high-risk items could have to the program.

Figure 1: Image of International Space Station **(***A world renowned laboratory in space enabling discoveries in science and technology that benefit life on Earth and exploration of the universe)*

The ISS Program implements two complementary processes, Continuous Risk Management (CRM) and Risk-Informed Decision Making (RIDM), which provide a foundation for proactive risk management throughout the program's lifecycle. The RIDM process is designed to facilitate and document the "risk-informed" selection of a decision alternative. The CRM process is set into motion once a decision has been made and requirements have been set.

RIDM is typically used when there are multiple solution paths to a problem and the alternative that is selected involves the base lining or changing of program requirements. The primary objective of RIDM is to provide the decision maker with the necessary risk information to make a decision that has the most potential of successfully meeting program objectives. CRM is designed to track and control identified risks associated with the alternative selected during RIDM, as well as to identify any new risks that may emerge once the alternative has been implemented. Risks that are managed via the CRM process (Figure 2) may warrant the need to change program requirements at some point in the future, thus providing input for an additional round of RIDM to re-baseline requirements.

The ISS Risk Management Application (IRMA) is the primary application used to support the ISS risk management process at Johnson Space Center (JSC). The system is used to document, track, manage, and mitigate risks, watch items, and concerns associated with

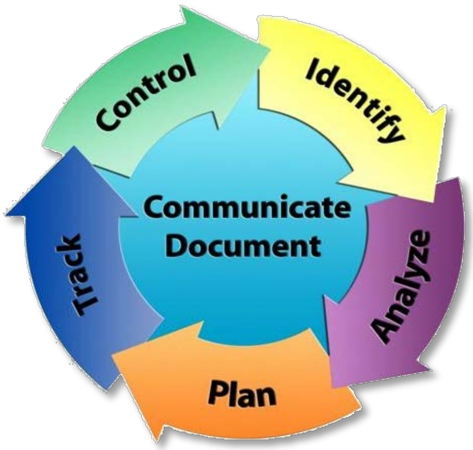

Figure 2: Continuous Risk Management Paradigm

the ISS Program. Once an issue is identified in IRMA, the risk owner enters the detailed information into IRMA for consideration by the initiating organization.

It is during the tracking process of CRM, that the ISS Program defines all possible mitigation steps needed to reduce the potential risk to the station and the crew. Each step has a specific description, responsible organization, defined start date, expected completion date, and resulting risk change upon completion of the step. The initiating organization weighs the information provided and decides whether or not, and how, the risk should be elevated to the appropriate level of management that may have the resources to mitigate the risk within the ISS Program.

Though there are several ways to assess the likelihood that an undesired event will occur, a Probabilistic Risk Assessment (PRA) is the most commonly used form of analysis in the ISS Program for determining a quantitative number for probability. PRAs can be performed for the risk analysis step of both the RIDM and CRM processes. A PRA may need to be supplemented by more detailed models to generate precise, or “tailored”, data that provides program management with the appropriate amount of risk-information to make specific decisions during the RIDM process. The two case studies below will demonstrate how detailed quantitative risk models were developed to further understand the risk and to identify the risk contributors in detail. Once the contributors are identified, you can then determine how to mitigate the risk more effectively.

PRA is a quantitative risk modeling approach that is a comprehensive, structured, and logical analysis method aimed at identifying and assessing risks in complex technological systems for the purpose of cost-effectively improving their safety and performance. NASA’s objective is to better understand and effectively manage risk, and thus more effectively ensure mission and programmatic success, and to achieve and maintain high safety standards at NASA (4).

This paper presents two case studies that will illustrate how the ISS risk management process has been used to address each specific area of risks.

2 Case Studies

2.1 Case Study 1: Meteoroid Orbital Debris Penetration

The ISS and its crew routinely face a series of potentially catastrophic risks due to MMOD. Impacts from MMOD present potentially fatal risks that, if realized, could injure the ISS crew members, force an evacuation of the ISS, or destroy the ISS and cause loss of the crew members in a large catastrophic event. As a result, MMOD penetration is considered a Top Program Risk by the Space Station Program Control Board and is monitored and analyzed both by the CRM and the RIDM processes.

2.1.1 Description of MMOD Risk

Negative consequences associated with an MMOD penetration can yield an evacuation of one (EVAC 3) or all six crew members (EVAC 6), loss of life of a crewmember (LOC), or loss of all crew and the ISS vehicle (LOCV). An MMOD strike leading to a slow depressurization of the ISS is the leading cause of EVAC 6. An MMOD strike that penetrates the ISS and strikes a crewmember could result in LOC, and the leading cause of LOCV is a MMOD strike that penetrates the ISS causing a rapid depressurization with insufficient time to take corrective actions or evacuate. Per the latest version of the ISS PRA model, the risk of MMOD penetration is the top driver for EVAC 6 and LOCV in a 6 month timeframe.

Figure 3 graphically illustrates the risk of MMOD in a six month time period. The risk of EVAC 6 due to MMOD penetration is 95% likely compared to Fire (3%) and loss of the Electrical Power System (1%). 56% of a LOCV scenario is due to a MMOD penetration compared to 44% due to a visiting vehicle collision. The risk of MMOD penetration is the 2nd top driver for an EVAC 3 (36%) and a LOC incident (38%) compared to the risk of a medical emergency at 60%.

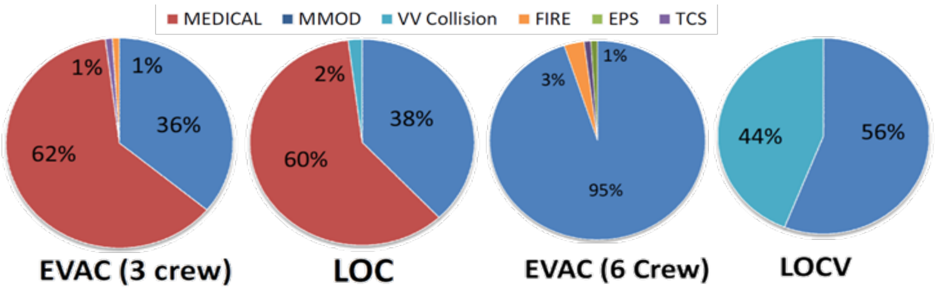

Figure 3: MMOD Penetration Risk in a 6 month period

As indicated by the LOC MMOD risk in Figure 4, the elements on the Russian Segment (RS) of the ISS (Progress, Service Module, Docking Compartment and Soyuz) and HTV posed larger threats of MMOD penetration due to the current MMOD protection and shielding pre-established methods. Since inadequate MMOD shielding on the RS can lead to a greater potential for MMOD penetration and depress contingencies, a RIDM effort has been put in place to change the ISS Program requirements to ensure further shielding and protection for these elements of concern.

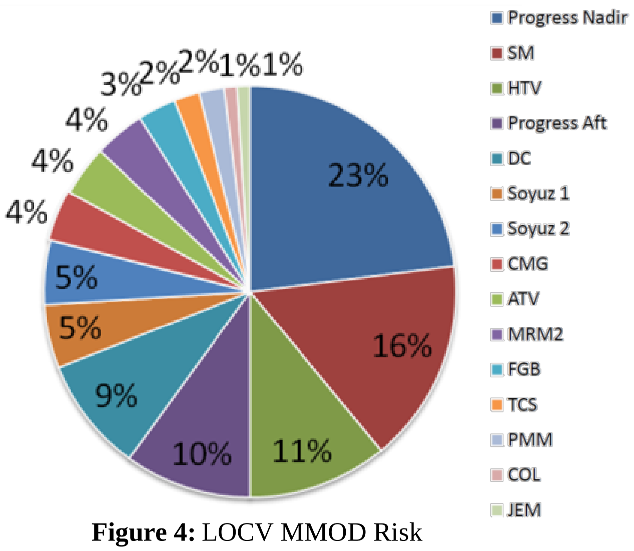

Figure 4: LOCV MMOD Risk

2.1.2 Basic Methodology

To support the CRM and RIDM efforts, "Integrated Threat Assessments have been performed to estimate the overall penetration risk from MMOD penetration and provide the risk results. The latest ITA, International Space Station Micrometeoroid and Orbital Debris Integrated Threat Assessment 12, was released in July of 2010. The NASA computer code BUMPER-II calculates the probability of no penetration for a spacecraft based on geometry, shielding configurations and flight parameters. The Manned Spacecraft Crew Survivability software code is a Monte Carlo simulator that generates orbital debris impacts based on the Orbital Debris Environment Model (ORDEM) 2000 environment (released in 2003), checks for penetration using critical diameters obtained from BUMPER-II, and in the event of a penetration checks for events resulting in the loss of at least one crew member." (4)

The analysis for this case study used the current MMOD environment modeled in ORDEM 2000, MEM 2.0 and applied a MMOD Uncertainty Methodology that can be used to predict the probability of zero penetrations, the probability of at least one penetrations and the expected number of penetrations to a module over time.

Assume that for a given module, with a failure rate equal to λ, the number of penetrations in time interval *t* follows a Poisson process (*i.e.*, the time between arrivals is exponentially distributed).

The probability of x penetrations to a given module in time *t* is described in as:

$$P(X=x)=\frac{(\lambda t)^{x}e^{-\lambda t}}{x!} \tag{1}$$

The probability of zero penetrations to a module is $P(X=0)=\frac{(\lambda t)^{0}e^{-\lambda t}}{0!}=e^{-\lambda t}$ (2)

The probability of at least one penetration to a module is $P\left(X > 0\right) = 1 - e^{-\lambda t}$ (3)

The expected number of penetrations to a module is $E\left(X\right) = \lambda t$ (4)

If the ISS has m modules, the probability of zero penetrations $P_{ISS}^{x=0} = \prod_{i=1}^{m} e^{-\lambda_i t_i}$ (5)

The probability of at least one penetration to the ISS is $P_{ISS}^{x>0} = 1 - \prod_{i=1}^{m} e^{-\lambda_i t_i}$ (6)

The expected number of penetrations to the ISS is $E_{ISS}\left(X\right) = \sum_{i=1}^{m} \lambda_i t_i$ (7)

Note: λ is the parameter of the exponential distribution and is assumed in this case to be lognormally distributed with a median values obtained from data for different locations. An Error Factor (EF) of 3.9 was used based on uncertainty associated with the estimated values. To determine the likelihood of MMOD penetration to the ISS, the λ for each module was sampled and 100,000 runs using ModelRisk were performed to obtain the final results.

2.1.3 Risk Impact to the ISS

A recent trade study was performed to calculate the probability of any MMOD penetration to the habitable volume of the ISS, for periods of six months and from 2013 (present day) to 2020 (end of life). This analysis used the current MMOD environment and ISS attitude to estimate the probability of future penetrations to the habitable volume of the ISS. The model included all applicable Russians and USOS modules including visiting vehicles and their estimated duration on the ISS during a six month period. The Automated Transfer Vehicle (ATV) was assumed to be on orbit three months out of six and the H-II Transfer Vehicle (HTV) was assumed to be on orbit one month out of six. A six month (180 day) timeframe was assumed to be 4,320 hours which was used as the run time for the first run of this study. For the second run of this study, the time period was between 2/04/2013 and 9/30/2020, which converts to 67,080 hours using Excel's CONVERT function.

To determine the risk of any MMOD penetration to the habitable volume of the ISS for a period of 6 months and from 2013 to 2020, the MMOD Uncertainty Methodology as described in section 2.1.2 was applied.

2.1.4 Case Study 1 Results

Case Study 1 results (Figure 6) revealed that the probability of MMOD penetration is fairly high within a six month period and slightly higher from now to the end of life. The mean, as indicated by the break point in the band-aid range representation for the MMOD probability of penetration in six months is 1 in 42 (2.4E-2) and is 1 in 4 (2.6E-1) for the probability of penetration between now and 2020. The range of the band-aid representation indicates the 95% uncertainty range.

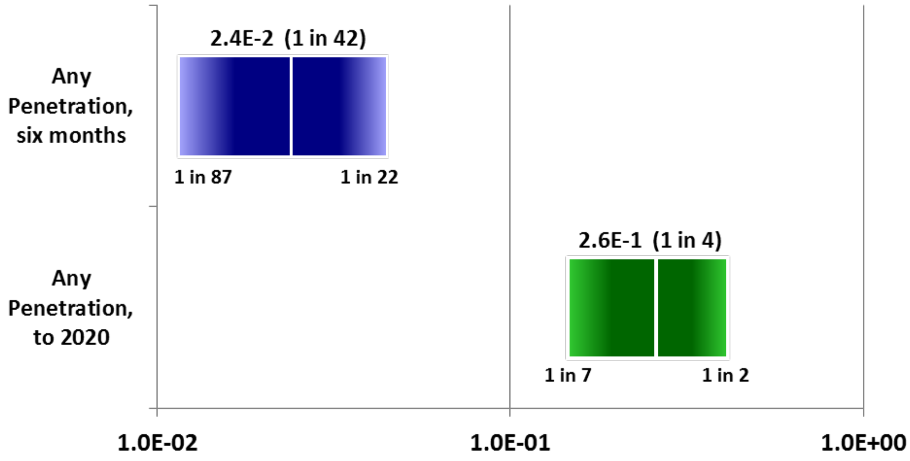

Figure 5: MMOD Penetration Probability (6 Months/End of Life)

2.1.5 Mitigation of MMOD Risk

NASA has developed a CRM process for dealing with the MMOD penetration risk. In 1995, an IRMA risk report was entered into the tracking system to address a lack of MMOD shielding on Russian flight elements. Inadequate MMOD shielding on the Russian Segment (RS) can lead to greater potential for MMOD penetration and depress contingencies.

While the risk of MMOD cannot be entirely eliminated, mitigation steps have been coordinated with the Russian Space Agency to help reduce the risk posed by the RS modules (SM, DC1 MRM1 and MRM2) and RS visiting vehicles (*i.e.*, Soyuz and Progress) as they have the highest risk of MMOD penetration, compared to other ISS modules.

To mitigate the MMOD risk, Hypervelocity Impact test findings are essential to MMOD risk assessments, design/verification of ISS MMOD shielding, functional failure assessments, support operations, and anomaly investigations. The ISS Program also continues to recalculate the 15-year Probability of No Penetration (PNP) for MMOD shielding of the ISS. RS estimated that additional MMOD shielding to the Service Module (SM), Progress, Soyuz and MRM 1 and 2 would help reduce the overall risk of MMMOD to the ISS. Figure 6 shows improved MMOD shielding that is currently installed on the Soyuz visiting vehicle. Recent installation of debris shields in 2012 to the SM decreased the risk by 15%.

As a part of the CRM process, the ISS Program continues to monitor the risk of MMOD penetration. Open communication, between the ISS Program and the Russian Space Program, has enabled NASA and International Partners to better understand and analyze the risk of MMOD penetration from now through the end of ISS. The ISS Program continuous monitoring of these areas occurs regularly at high level Program Risk meetings where all organizations perform a continuous assessment of risks and strategize ways to mitigate those risks.

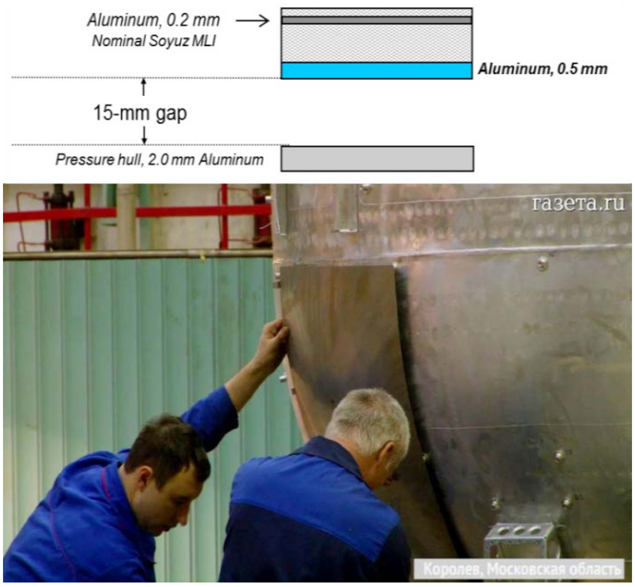

Figure 6: Improved Soyuz MMOD Shielding

2.2 Case Study 2: ISS Visiting Vehicle Collisions

The ISS uses the capabilities of different space vehicles to launch flight elements, systems for assembly, utilization and resupply items, and crew to orbit. Space vehicles of various designs are envisaged to be developed in support of these functions (5). These vehicles, which visit the on-orbit Space Station, are generally called Visiting Vehicles (VVs).

The ISS Program is continuously modeling and quantifying the catastrophic risk of collision from VVs. Given the right conditions during a VV docking or berthing (wherein the robotic arm assists vehicles who attach/connect to the ISS), there is a possibility of a collision occurring with the ISS and the program must remain aware of this concern and implement all possible mitigations and controls to prevent this catastrophic hazard.

2.2.1 Description of Visiting Vehicle Risk

As the ISS enters a new era of visiting vehicle traffic, including governmental (Automated Transfer Vehicle (ATV), H-II Transfer Vehicle (HTV), Soyuz, and Progress) and commercial cargo for unmanned resupply services (SpaceX Dragon® and Orbital Cygnus®), the ISS Program will have to withstand increased risk to the space station in the form of visiting vehicle collision. During the VV approach and departure mission profile, there is an increased likelihood of collision with the ISS due to its close proximity with the space station.

To understand the overall risk to the ISS and crew, VV spacecraft rendezvous, docking, and undocking scenarios were developed for each visiting vehicle and incorporated into the ISS PRA model. Risk associated end states modeled in this case study included Loss of Mission (LOM), Loss of an ISS Docking Port (LOP), likelihood of an abort, and likelihood of collision with the ISS (which results in Loss of Crew and Vehicle (LOCV)). While all of these consequences are significant, the likelihood of ISS collision due to a visiting vehicle is the only risk-associated end state that leads to EVAC, LOC, or LOCV and is likewise of interest to the ISS Program. As noted from case study 1, the risk of ISS Collision due to a VV is the second highest contributor to LOCV in the current ISS PRA Model.

2.2.2 Basic Methodology

The ISS program currently ranks the risk of visiting vehicle collision as a major concern for the ISS program. A comprehensive PRA is necessary to quantitatively capture the integrated risk contribution to the ISS from visiting vehicles during a 6 month period. Each visiting vehicle's collision hazard is assessed per mission, and necessary controls are implemented throughout the safety review process. These controls are incorporated into vehicle systems designs, and are modeled in the PRA model for each VV.

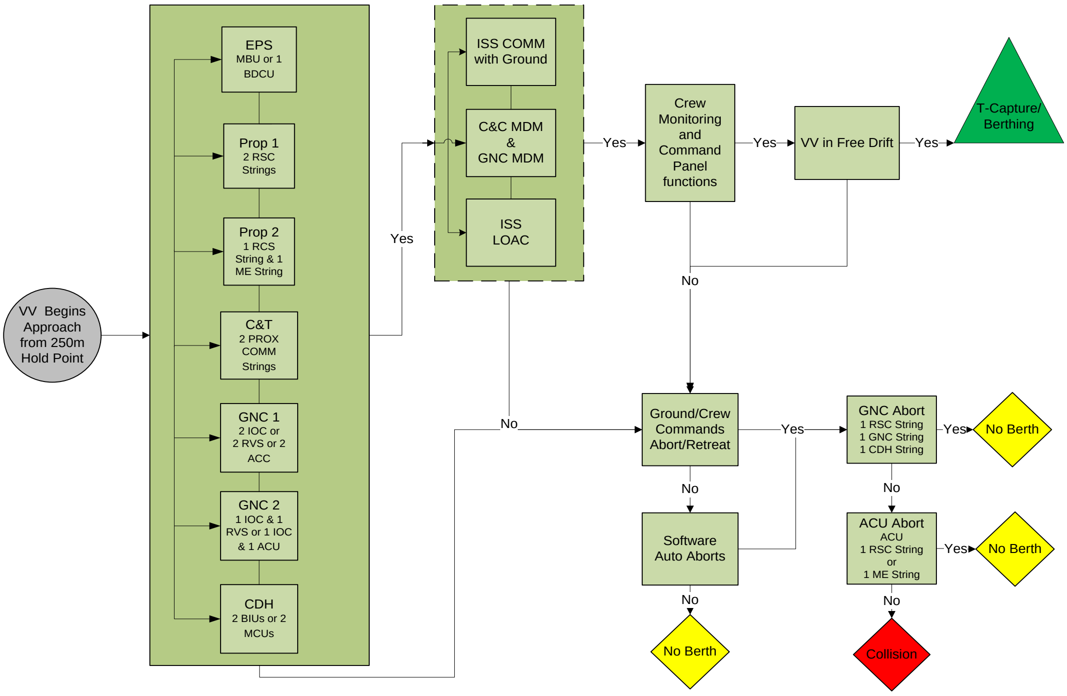
VV Begins Approach from 250m Hold Point
EPS MBU or 1 BDCU
Prop 1 2 RSC Strings
Prop 2 1 RCS String & 1 ME String
C&T 2 PROX COMM Strings
GNC 1 2 IOC or 2 RVS or 2 ACC
GNC 2 1 IOC & 1 RVS or 1 IOC & 1 ACU
CDH 2 BIUs or 2 MCUs
Yes
ISS COMM with Ground
C&C MDM & GNC MDM
ISS LOAC
No
Yes
Crew Monitoring and Command Panel functions
Yes
VV in Free Drift
Yes
T-Capture/ Berthing
No
Ground/Crew Commands Abort/Retreat
Yes
GNC Abort 1 RSC String 1 GNC String 1 CDH String
Yes
No Berth
No
Software Auto Aborts
No
No Berth
No
ACU Abort ACU 1 RSC String or 1 ME String
Yes
No Berth
No
Collision

Figure 7: Generic Visiting Vehicle Event Sequence Diagram

SAPHIRE is an integrated PRA software tool that gives a user the ability to create and analyze fault trees and event trees using a personal computer (9). Full-scale visiting vehicle models were developed in SAPHIRE, independently for the Soyuz, Progress, ATV, HTV, Dragon and Cygnus visiting vehicles. The analyzed results were used as a part of the integrated ISS PRA SAPHIRE model to determine the likelihood of negative end states to ISS. This allows the analyst to assess and quantify the contribution of each visiting vehicle to the overall risk of collision to the ISS.

Event Sequence Diagrams (ESDs), illustrated in Figure 7, were developed for each visiting vehicle to show the individual system(s) interdependences and how a certain sequence of scenarios leads to an undesired end state (9). The undesired end state resulting in immediate harm to the ISS is indicated by the red diamond. In the example provided below, the visiting vehicle is in the approach phase of flight, 250 kilometers from the ISS. To realize a collision end state, a series of core system failures on both the prime and redundant string need to occur and the vehicle's independent abort system needs to fail.

The next step in the modeling process involved developing the individual system logic using fault trees and event trees. Fault trees are logical representations of the credible failures that can cause an undesired event to occur. Figure 9 illustrates a fault tree for a visiting vehicle's abort system in which all Guidance, Navigation and Control (GNC) computers need to fail and both the prime and redundant Propulsion strings would need to fail to result in the inability of the system to perform a nominal GNC abort using either String 1 or String 2.

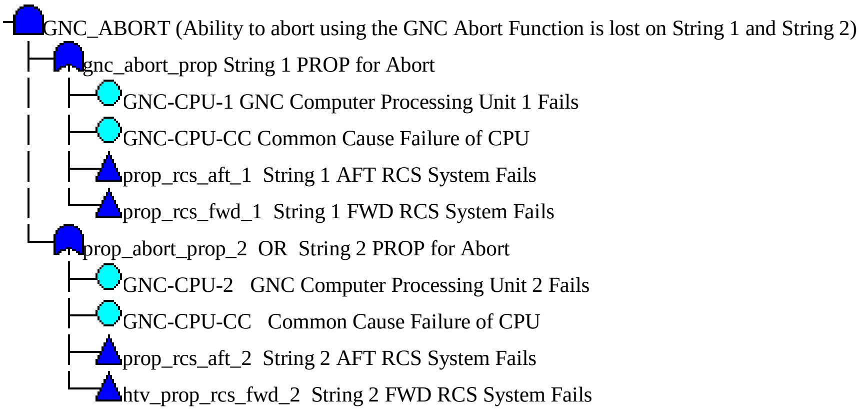
GNC_ABORT (Ability to abort using the GNC Abort Function is lost on String 1 and String 2)
gnc_abort_prop String 1 PROP for Abort
GNC-CPU-1 GNC Computer Processing Unit 1 Fails
GNC-CPU-CC Common Cause Failure of CPU
prop_rcs_aft_1 String 1 AFT RCS System Fails
prop_rcs_fwd_1 String 1 FWD RCS System Fails
prop_abort_prop_2 OR String 2 PROP for Abort
GNC-CPU-2 GNC Computer Processing Unit 2 Fails
GNC-CPU-CC Common Cause Failure of CPU
prop_rcs_aft_2 String 2 AFT RCS System Fails
htv_prop_rcs_fwd_2 String 2 FWD RCS System Fails

Figure 8: Fault Tree for a Generic Visiting Vehicle Abort System

Event trees were developed to model the sequences involving the initiating events and necessary failure occurrences (9). The fault and event trees were then linked together to estimate the likelihood of an undesired end state.

2.2.3 Risk Impacts to ISS

Figure 9 shows the current estimated probability of collision for each visiting vehicle. In a generic six month period, 2 Soyuz, 3 Progress, 1 HTV, 1 Dragon and 1 Cygnus are expected to approach ISS. To estimate the probability of collision, 8 approach attempts were modeled to obtain the overall 6 month risk. In general, the probabilities of collision for each visit of each vehicle were within an order of magnitude of each other. When all 8 approaches are modeled, the total risk of visiting vehicle collision increased by approximately an order of magnitude.

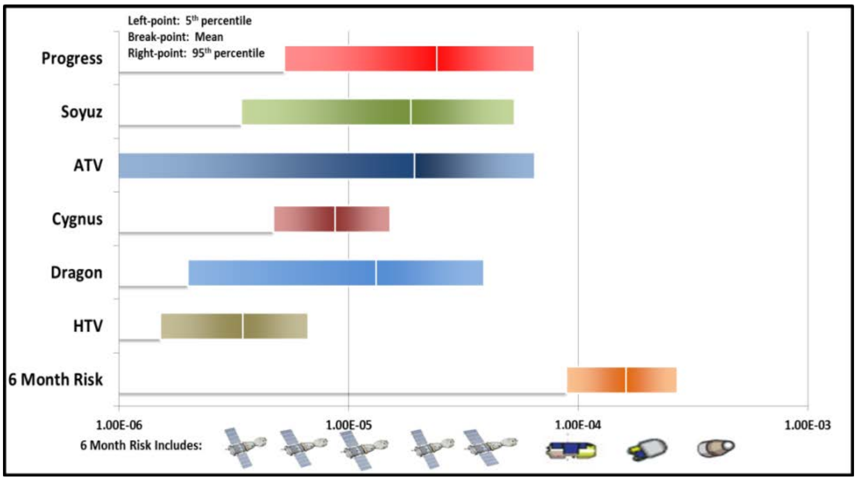

Figure 9: Six Months Risk of Visiting Vehicle Collision

2.2.4 Mitigation of Visiting Vehicle Risk

Applying the CRM process, the risk of visiting vehicle collision was first identified as a possible issue of concern in early 2012. Given the increased visiting vehicle traffic planned to ISS, there is an increased probability that a VV collision may occur resulting in a catastrophic loss of crew and vehicle (8). Prior to implementing risk mitigation strategies, the risk must be understood through analysis, planned for in operational procedures, system/software design and hazard controls and accepted by the ISS Program. The main objective of this IRMA entry in the tracking database was to increase awareness of this issue from visiting vehicle collision and develop risk mitigation strategies to reduce the risk. The ISS Program recognized the need to rank areas of concern and to keep a list of potential issues that may impact the continued success of the station.

As a part of the CRM process, the PRAB recently reviewed the results provided by the ISS PRA Team. It was determine that all required hazard controls, operational controls, system fault tolerances and safety measures defined per NASA safety requirements were properly accounted for and implemented in all five visiting vehicle system architecture and operational procedures. Based on the PRA results, the ISS Program as well as the ISS Safety and Mission Assurance Chief Safety Officer recommended that additional mitigation steps were not required. The Program and safety members felt the risk mitigations put in place during design and development of operational controls were adequate and there was no benefit in mitigating this risk further.

3 Conclusion

NASA continues to conduct CRM and RIDM for the ISS Program by proactively identifying, analyzing, and mitigating risks of potential areas of concern. The ISS Program continues to evolve as concerns arise during the life of the program, and are assessed for their likelihood of occurrence and consequences, and to identify mitigating measures where they are deemed necessary. The two case studies illustrate the application of the CRM and RIDM processes to the MMOD and visiting vehicle collision risks.

References

[1]. A Global Approach to Fisk Management: Lessons from the Nuclear Industry. Kaufer, B. and Lazo, T. No. 21.1, s.l.: NEA NEWS, 2003, Vol. Facts and Opinions.

[2]. ISS Risk Management Plan. Houston: International Space Station, 2009. SSP 50175.

[3]. Stamatelatos, M. and Dezfuli, H. Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners. Washington DC: NASA, 2011. NASA/SP-2011-3412.

[4]. IRMA Documentation - MMDO. s.l.: Johnson Space Center, 2005.

[5]. Interface Definition Document (IDD) for International Space Station (ISS) Visiting Vehicles (VVs). s.l.: International Space Station, 2000. SSP 50235.

[6]. Paranoid Risk Management - Ways to Remove Pitfalls and Fears of Risk Management. Croskery, K., Kraus, C. and Brown, P. 2008.

[7]. Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects. 2010. NASA Procedural Requirement, NPR 8705.5A-TOC.

[8]. IRMA Documentation – Potential Visiting Vehicle Collision with ISS. s.l.: Johnson Space Center, 2012.

[9]. Smith, C., Knudsen, J., Wood, T. Advanced SAPHIRE: Modeling Methods for PRA via SAPIRE Software. Idaho National Laboratory. February 2009.

K. L. Carter-Journet is a Technical Analyst III at ARES Corporation, where she supports Safety and Mission Assurance at Johnson Space Center to assess program risk for the International Space Station (ISS). She has a Bachelor's Degree in Physics from Southern University in Baton Rouge, Louisiana and a Master of Science in Biophysics from Cornell University in Ithaca, New York.

J. A. Calhoun is a Technical Analyst II at ARES Corporation, where she supports Safety and Mission Assurance at Johnson Space Center to assess program risk for the International Space Station (ISS). She has a Bachelor's Degree in Aerospace Engineering from Georgia Institute of Technology in Atlanta, Georgia and a Master of Science in Systems Engineering from the University of Houston Clear Lake in Houston, Texas.

M.G. Lutomski is an aerospace engineer with close to three decades of experience in Human Spaceflight including the Space Shuttle and International Space Station programs. Mr. Lutomski retired from NASA in 2013 and is currently the Director of Risk and System Safety at Space Exploration Corporation. He has a Bachelor's of Science degree in Aerospace Engineering from the University of Michigan and a Master's in Business Administration – Finance from the University of Houston's C.T. Bauer College of Business.

M. R. Raftery is a Risk Integrator at ARES Corporation, where he supports Safety and Mission Assurance at Johnson Space Center by implementing and maintaining the risk management processes for the International Space Station (ISS) Program. He has a Bachelor's Degree in Industrial Engineering from Texas A&M University in College Station, Texas.