Experience Gained from Developing a PRA During the Design Phase of NASA Human Exploration Missions

Diana L. DeMott*[a], Roger L. Boyer[b], Mark Bigler[b], Courtenay B. Clifford[a], and C. Joseph Kahn[a]
[a] SAIC, Houston, Texas, USA
[b] NASA, Houston, Texas, USA

Abstract: NASA human space programs use Probabilistic Risk Assessment (PRA) to identify and quantify mission risk. This paper discusses some challenges and benefits for developing a PRA early in the development phase for a complex project involving multiple programs with different schedules, goals and management. This is based on experience gained by NASA Safety and Mission Assurance (S&MA) supporting the NASA Exploration System Development (ESD) Programs (major components include Orion, Space Launch System, and Ground Systems) over the last several years. Included is a summary of different aspects of a space mission PRA, overview of the integration experiences encountered as NASA develops a Cross Program PRA (XPRA) pulling individual program level PRAs together for a complete PRA for the first human exploration mission beyond Low Earth Orbit in 50 years and the issues involved in the management and implementation process given a variety of partners and organizations involved. Other benefits and challenges discussed include: preliminary design requirement risk validation, using Risk Informed Decision Making (RIDM) as a management tool, interfacing with different organizations with different user needs for PRA results, dealing with data issues, integrating multiple designs and assessment philosophies from different organizations, and incorporating flight dynamics with multiple failure scenarios.

Keywords: PRA, integrated PRA, multi-program PRA, space applications

1. INTRODUCTION

A PRA for a space mission addresses multiple failure scenarios caused by a variety of failure events that can occur during different environments and dynamic events (pre-launch, ascent, low Earth orbit (LEO), cis-lunar space, Entry/Descent/Landing (EDL) and post-landing). Using PRA in the early design phase has the potential to improve the design of systems and the vehicle by reducing the probability for events that could lead to Loss of Crew (LOC) or Loss of Mission (LOM). LOC and LOM have been defined as the end states of interest to NASA for human space missions. The intent of performing these assessments in the design phase is to improve safety by identifying the top risk contributors leading to improvements in design, operation, and maintenance. Other potential benefits include: enhancing probability of mission success, improving system performance, reducing costs for design, operation and maintenance. NASA applies a Risk Informed Decision Making (RIDM) [1] process intended to assist management in setting priorities for resource allocation and optimize results for given resource availability. These priorities can be met by providing additional risk information to assist in enhancing design decisions, mission decisions, administrative policies, equipment, program contracts, processes, procedures, and training.

2. CURRENT STATUS OF NASA EXPLORATION SYSTEM PROGRAM

The ESD programs have completed the initial design phase using design reference mission requirements, mission specifications, and incorporating previous experience in the development and operations of human missions to integrate the various program PRAs into the "Cross Program" PRA (XPRA)[2]. Having different organizations and NASA Centers responsible for various aspects of program and vehicle development has led to a number of challenges in developing the XPRA. Since this endeavour encompasses multiple programs, companies and projects that are developing designs based on their specific project requirements, specifications and goals, each program has developed

*SAIC, Houston, TX, USA; email: diana.l.demott@nasa.gov

their own assessments to meet their specific requirements. The goal of the NASA XPRA team (XPRAT) is to develop a PRA that encompasses all the aspects of the mission needed to produce a single PRA that describes the entire mission in as consistent a manner as possible. Some of the integration issues identified include: establishing a common methodology [2], managing different assumptions and priorities, schedule concerns, modeling philosophies, different modeling techniques, and dealing with different interpretations of the same requirements. The following discussions identify several expected and unexpected situations experienced.

3. INTEGRATION EXPERIENCES

3.1. Overview

Each NASA program and project has been authorized to develop its own PRA to verify compliance with their own program specific LOC and LOM requirements. XPRAT was tasked with integrating all the program and project work into an overall mission PRA (represented as the XPRA in the following discussions). Although XPRAT established the use of a common methodology, nothing is ever perfect and due to various reasons (contracts, subcontracts, program analyst preferences, etc.), some deviations or inconsistencies in applications of the methodology exist. As discrepancies have been identified, PRA program teams have worked together to resolve these inconsistencies or document the issues for possible future evaluation. Some of the challenges experienced with a integrating a multi-program PRA include, but are not limited to: identifying a method to adequately describe differences in flight dynamics based on mission phase (ascent, ascent and in-space aborts, LEO, cis-lunar, EDL, how to use naming conventions in the model to enhance usefulness of results, and integrating multiple designs from different organizations that used different assumptions, data and modeling philosophies.

Since the goal of the PRA is to provide a risk assessment for the defined exploration mission, keeping management informed during the development and design process is also a priority and has also produced some interesting "lessons" that include: dealing with time lags for results and design/mission changes, responding to management requests, presenting or communicating results effectively to management, operations, and engineering, and influencing management decisions.

3.2. Conceptual and Preliminary Design Experiences

Developing a PRA for equipment, processes and operating systems that are in concept or preliminary design phases involves additional challenges in PRA modeling. In order to develop a human space mission PRA to be used in improving crew safety and categorizing vehicle risk during the concept and preliminary design phases, a variety of assumptions needed to be identified as a starting point. Examples of these assumptions include:

- Assuming a best-estimate risk assessment approach versus design safety limits used by engineering to design the vehicles.
- Identifying reasonable assumptions as placeholders during early state of knowledge for a Design Reference Mission (DRM) concept of operations. The DRM concept of operations usually lags several years before maturity, so the PRA team assumptions need to fill knowledge gaps until programs mature to provide the requisite knowledge. As vehicle and mission designs and operational plans mature, the state of knowledge increases and changes. Future iterations of the XPRA will continue to changes or elimination assumptions as information becomes available.
- The model assumes current known design capability has been achieved (i.e. constant failure rates on the flat part of the reliability bath tub curve). The PRA is not used to assess early or first flight risk. To do so, requires a different approach that is not part of this discussion. Constant failure rate in most cases (exceptions as needed) is time-averaged based on model parameters.
- Preliminary Design documents include: technical specifications and requirements, system design requirements and/or diagrams, Operations experience, Ground Support experience, "System/Domain" Experts, analysis reports, design reference mission requirements, etc.

Since one of the goals for developing an integrated model early in the design phase has been to identify and reduce risk, one of the early efforts was to establish risk requirements as a basis for measurement. Setting risk requirements in the preliminary design phase has been challenging. Using results from previous NASA programs (such as the Space Shuttle and the International Space Station, ISS) to establish requirements for LOC and LOM must be done carefully when PRAs based on more detailed design and operations are performed. One area of particular difficulty is the task of setting risk requirements based on mission phase. Issues can arise due to a number of factors including scenarios involving failures that occur over multiple phases, where the risk is initiated versus where it is realized, definitions of the start and end of the phase, and other program specific concerns. Trying to establish requirements based on phase can also be complicated by the fact that the missions can vary significantly in length and profile. Using the PRA as a risk-informed decision tool to help guide the design does not produce the same concerns.

3.3. Implementation and Integration Experiences

The XPRA uses event trees representing mission phases to incorporate program interfaces and major mission events using the systems analysis tool SAPHIRE [3]. Individual program PRAs and other data provided by team members were entered into the event tree construct through the use of fault trees and basic event data. When combining the failure logic from different teams to give an overall characterization of the risk associated with a mission, care should be given to the differences that each organization used in developing the PRA for their contributions to the total mission. Sensitivity studies may be needed to identify the consequences of these different approaches and to determine if modifications may be necessary. Observed differences between PRAs included failure data estimation, level of model detail, use of off-line models, definition of correlation classes, and the methods used for common cause. Some of the issues encountered include:

- Approach to developing PRA models were based on NASA procedures guides [2][4][5]. However, there were differences between PRA program source models being incorporated into the XPRA due to:
    - Models from different NASA Programs, each with its own modeling team used the same guidelines when constructing their PRAs but sometimes reached different interpretations for their modeling approaches.
    - The level of model detail varied based on the information available or the assumptions used by each PRA modeling team.
    - In some cases, off-line modeling was used to develop results for systems or programs. However, off-line models representing vehicle systems or components could ignore details and logic representing that part of the system analyzed off-line and could result in missing some of the relationships between components in other systems. Off-line models, such as the crew medical model (or health risk of being a human over the duration of the mission), are independent of the vehicle model.
    - Different programs used different interpretations of Common Cause Failure (CCF) methodologies or different parameters in development of their models. Observed variations of the approach include: 1) using different CCF alpha factor NUREG [6] updates can create questions if different programs update while others use earlier versions, 2) defining a common cause group to include all identical components in the system or including only redundant components and, 3) grouping common cause events under a single fault tree at a system level in the model or including CCF failure rates at individual component levels. If the same component is used across systems, this allows for the potential for the same component CCF to be assessed differently in different program models.
    - Some programs used the compound event feature in order to capture the uncertainties of both the independent event and the common cause parameters within SAPHIRE. Other programs calculate the common cause events as data development and then put

them into the SAPHIRE models. This could create questions on the overall uncertainties associated with these events.
    - Estimations for software failure rates have also been performed using different tools. This can create questions regarding how similar the results would be if the same tool was used for both programs and how the two numbers would compare.
    - Current review efforts indicate that the effect of these deviations on the total mission risk is negligible. Additional reviews may occur in the future.
- Approach to Failure Data Development differed based on:
    - Failure data from generic historical data sources to determine a generic prior and distribution uncertainty. Bayesian methods are then applied to the generic prior to update the value with more current information if it exists. The basic event time parameter is the duration of the specific mission phase.
    - Single point failure data derived from internal and external sources. Various factors (e.g., environment, common cause, demands, failure mode, etc.) are applied to the phase time parameter.
    - Data used for similar failures could be quite different in the program models that are used as input to the XPRA. Current review efforts indicate that the effect of these deviations on the total mission risk is negligible. Additional reviews may occur in the future.
- Approach to Uncertainty Calculation used the methodology in "Office of Safety and Mission Assurance (OSMA) PRA Procedure Guide" [4] and NUREG-1855 [7]. These documents were used by each program, however, different approaches to defining the uncertainty parameters of the failure estimate such as distribution type and correlation class were made which affected how results could be included in the SAPHIRE software. The differences in defining the uncertainty parameters was:
    - The majority of the participants calculated uncertainty using SAPHIRE which is based on distribution type and distribution characteristics to the failure data of each basic event. The distribution type was typically lognormal, and its error factor calculated using standard statistical methods applied to the data used to determine the failure probability. All Basic Events that derive their failure probability from the same data were assigned to the same correlation class.
    - Another group used an approach that included assigning a standard error factor based on the technical readiness of the component rather than the statistical methods and assigning a unique correlation class to each basic event across the modelled phases. While these unique classes should result in a lower calculated uncertainty, its effect is generally not discernible at either the overall or system level results.
    - Current review efforts indicate that the effect of these deviations on the total mission risk is negligible. Additional reviews may occur in the future.

3.4. Model Integration Experiences

PRAs typically model large/complex systems down to the level of where data exists. This is essential in reducing engineering 'guesswork' about the likelihood of failure at the system level. Because of the dynamic nature of preliminary design efforts, each program had different design review schedules with their associated PRAs tied to their program specific schedule. Because modeling design changes takes time, PRA results often reflected a design that was out of date by at least one review cycle. This was often the result of not being in a position to sync the various design and analysis review cycles which were set by each program participant. Program preliminary and critical design review milestones have different deliverable schedules, resulting in the XPRA having different levels of maturity depending on the program. For example, the Orion vehicle has been in development since 2006 and further in the design, while new launch facility designs need to be developed to support the evolving SLS booster design.

The XPRA uses results reviewed and approved by each program's management in the latest iteration. However, work on the program PRAs continues at the same time the latest version of the XPRA is being assembled. This can cause the XPRA to include inputs that are out of date when compared to individual programs updates. This can result in differences in the results shown to program management and thus generate confusion. Ideally, the integrated model would have a sufficiently fast turnaround time to keep the integrated model current with all the progress made in each program. However no easy solution for this has been discovered, so the XPRA model will continue to have a time lag in assessing the latest design modifications.

Other considerations that reflected how interpretations and initial planning affected the model included the following:

- XPRAT used Idaho National Laboratory's SAPHIRE 7 PRA program for model integration, which was the current version at the beginning of the XPRA effort. This has resulted in the vast majority of a very large and complex XPRA model using this version of SAPHIRE. Like any software, SAPHIRE has continued to be updated, and eventually a new SAPHIRE 8 version was issued. Version 8 was essentially a re-write of the program with an entirely new user interface. While most of the NASA PRA community continues to use the established SAPHIRE 7, some users have begun to take advantage of the newer program's interface advantages and its evolving capabilities. Comparisons of the two versions of the software to verify that results would be the same regardless of which model is used have not been performed. The change to SAPHIRE 8 is under consideration.
- NASA also attempted to recreate fault trees built by a program partner who developed the fault trees using a different fault tree software program. A discrepancy, although not large, was identified re-enforcing the need for caution with trying to integrate models from different software programs.
- The naming scheme determines the ease, and even the possibility, of how a model's results can be reported. Since reporting risk drivers is a valuable asset for management and Risk Informed Decision Making (RIDM) [1], the capability of a PRA to rank and relate these types of risks that make up the results is beneficial. Therefore, before modeling began, extensive thought was given to how the model's cut sets might be grouped in a report and communicated to management. Of course, there are challenges in crafting a usable naming scheme when multiple modelers are involved, which are greatly multiplied when the development team is spread among multiple centers, multiple contracting companies, and multiple time zones. The XPRAT produced a common methodology which addressed the naming scheme. As the vehicle designs and operation matured over the years, so did the corresponding PRA and the need to update the original naming scheme as new items came to light.
- Although the XPRA uses most models "as is", some models had to be extended for incorporating the information into additional phases of the mission, or to analyze other missions. Therefore, the integration team developed a spreadsheet data base with an entry for every basic event in the extended model. This spreadsheet can be directly imported into the SAPHIRE program allowing for faster data input and an easier method for performing sensitivity studies using different reliability data.

3.5. Other Considerations

The original PRA model was developed using a specific Design Reference Mission (DRM). As the program has matured, the potential for changes to the DRM are under consideration and can have either limited or substantial effect on model accuracy and effectiveness depending on how the DRM is changed.

The use of assumptions is always needed when developing a PRA model, however, when creating a PRA model for a preliminary design encompassing new technologies and postulated failure scenarios, this consideration becomes even more important. From an integration standpoint, the most pressing issues identified have been:

1) Assumptions made by individual programs can overlap. As each program has developed their designs, they have often made certain assumptions regarding what or how another program would interface with their design. These assumptions when compared across programs don't always prove to be accurate. Additional efforts to keep track of and verify assumptions made regarding other programs remains difficult. As a result, the XPRA does its best to resolve these differences and provide a more realistic assessment across the programs.
2) Given the dynamic nature of the changes made when developing a PRA while the design process is in progress, providing detailed documentation regarding the reasons and rationale behind assumptions allows for a more reasonable review and validation process.

Sensitivity runs and results, have been used effectively to provide management with additional information on design changes. However, determining what sensitivity runs are most useful requires greater interaction with design and operations groups who may not be aware of the potential uses for these tools.

Given the transitional nature of a PRA associated with preliminary design information that progresses through multiple iterations, documentation is essential. The following information should be included for each iteration developed: 1) all assumptions and design details associated with the model based on specific design parameters, 2) any tools used in developing charts, spreadsheets or calculation aids, 3) any additional information allowing a reviewer to generate reproducible results, which includes interpretations and definitions used by the analyst, and 4) list of any supporting analysis workbooks or referenced white papers. Any specific software tools used should be archived and documented for future retrieval.

Reporting results has shown a "learning curve" as different management personnel becomes exposed to the concepts and methodology as the results are presented. Therefore, XPRAT learns what each customer or management team is looking for and understands best. Over time, management personnel have slowly been exposed to the concepts and methodologies used in PRA, and this knowledge growth by management personnel has also assisted XPRA in providing more meaningful results. The trick remains to ensure that the PRA team effectively communicates the results to the right management.

4. CONCLUSION

The purpose of the XPRA is to support crew safety and verify NASA Safety and Mission Assurance requirements are being met. However, it also provides management with additional tools for decision making, can assist in performing risk trade studies and ultimately provides a methodology for identifying and mitigating risks for a high risk environment that is based on new and evolving technologies and equipment.

Despite all of these challenges, experience has shown that utilizing PRA in the development and design phases has been very beneficial, and the XPRA has actually had a positive impact on the safety of the design and operations. Many of the issues identified during this integration process are applicable to any complicated large scale PRA with multiple partners and different organizational priorities who want to identify and quantify vulnerabilities and risks in early design phases.

Acknowledgements

The NASA teams supporting the PRA (Space Launch Systems PRA, Lockheed Martin Orion PRA, Exploration Ground Support, NASA Human Health and Performance, Safety and Mission Assurance Analysis, SAIC PRA, and Flight Operations Directorate) are composed of dedicated groups of

individuals who are invested in providing tools and information that enhances the safety and success of space exploration.

References

[1] Homayoon Dezfuli Michael Stamatelatos, Gaspare Maggio, Christopher Everett and Robert Youngblood, *"NASA Risk-Informed Decision Making Handbook, NASA/SP-2010-576,Version 1.0"*, Office of Safety and Mission Assurance, Washington, D.C., April 2010

[2] "Exploration Systems Development Safety and Mission Assurance Plan" ESD 10010, rev. B, National Aeronautics and Space Administration, March 2016

[3] S. T. Wood, C. L. Smith, K. J. Kvarfordt and S. T. Beck, *"NUREG/CR-6952, Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Vol. 1 Summary Manual,"* Idaho National Laboratory, Idaho Falls, ID, September 2008

[4] M. G. Stamatelatos and H. Dezfuli, "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, NAS/SP-2011-3421, Second Edition," Office of Safety and Mission Assurance, Washington, D.C., December 2011.

[5] Michael Stamatelatos and José Caraballo, *Fault Tree Handbook with Aerospace Applications*, NASA Office of Safety and Mission Assurance, Washington, DC 20546, August, 2002

[6] U.S. Nuclear Regulatory Commission, "CCF Parameter Estimations, 2012 Update", Washington, D.C., November 2013

[7] U.S. Nuclear Regulatory Commission, "Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making, NUREG-1855, Vol. 1", U.S. Nuclear Regulatory Commission, Washington, D.C., March 2009