2009 Space Shuttle Probabilistic Risk Assessment Overview

Teri L. Hamlin[a*], Michael A. Canga[a], Roger L. Boyer[a], and Eric B. Thigpen[b]
[a] National Aeronautics and Space Administration (NASA), Houston, USA
[b]Science Applications International Corporation (SAIC), Houston, USA

Abstract:

Loss of a Space Shuttle during flight has severe consequences, including loss of a significant national asset; loss of national confidence and pride; and, most importantly, loss of human life. The Shuttle Probabilistic Risk Assessment (SPRA) is used to identify risk contributors and their significance; thus, assisting management in determining how to reduce risk.

In 2006, an overview of the SPRA Iteration 2.1 was presented at PSAM 8 [1]. Like all successful PRAs, the SPRA is a living PRA and has undergone revisions since PSAM 8. The latest revision to the SPRA is Iteration 3.1, and it will not be the last as the Shuttle program progresses and more is learned.

This paper discusses the SPRA scope, overall methodology, and results, as well as provides risk insights. The scope, assumptions, uncertainties, and limitations of this assessment provide risk-informed perspective to aid management's decision-making process. In addition, this paper compares the Iteration 3.1 analysis and results to the Iteration 2.1 analysis and results presented at PSAM 8.

Keywords: PRA, Shuttle, LOCV

1. INTRODUCTION

The National Aeronautics and Space Administration (NASA) initially used Failure Modes and Effects Analysis as well as Hazard Analysis to understand the risks associated with Space Shuttle flight. These assessments were useful to identify the many risks inherent in the design and operating environment of the spacecraft, and the assessment results could be used to inform recommendations for improving the design and operational risk controls. However, the qualitative nature of these assessments can lead to inconsistency and imprecision in risk characterization that make risk prioritization difficult and risk aggregation impossible. For these reasons, it was not historically feasible to derive a robust Shuttle reliability estimate or to accurately prioritize top risk contributors. Such insight is crucial to improving the reliability of the Space Shuttle system.

With this in mind, the Space Shuttle Program (SSP) initiated the development of the SPRA to provide a useful risk management tool for identifying strengths and possible weaknesses in the Shuttle design and operation. The SPRA model is a typical PRA model in that it is based on fault trees and event trees populated with failure rate and probability data. However, it is unique because of the dynamic nature of the mission and environment it models.

Like all successful PRAs, the SPRA is a living analysis. The latest revision to the SPRA is Iteration 3.1, and it will not be the last as additional risk insight is gained about the Shuttle and used to support subsequent Shuttle flights. This paper provides the SPRA Iteration 3.1 analysis and results and compares them to those previously presented in 2006 as SPRA Iteration 2.1 [1]. The SPRA has undergone two minor revisions and one major revision since PSAM 8. The minor updates included the addition of on-orbit inspection/repair and crew rescue. These features were added to program

* *Teri.L.Hamlin@nasa.gov*

capabilities and subsequently reflected in the integrated SPRA model following the Columbia accident to mitigate the risk of Thermal Protection System (TPS) damage resulting from ascent debris and Micrometeoroid and Orbital Debris (MMOD) impacts. Other minor updates also corrected errors detected in the previous version of the SPRA model. The major update expanded the SPRA scope to include benign engine shutdown and stuck throttle aborts during ascent as well as rendezvous and docking operations in orbit. Including aborts significantly increased the complexity of the SPRA model but the added risk was minimal, less than 1%. The major SPRA update also included a re-evaluation of the data.

2. SCOPE

The SPRA includes hazards that may result in an in-flight Loss of Crew and Vehicle (LOCV). In-flight is defined as the time from liftoff (T-0) to wheel stop. As previously mentioned, Iteration 3.1 has expanded the scope of a "nominal" mission, as compared to Iteration 2.1, to include rendezvous and docking with the ISS as well as ascent aborts. Rendezvous and docking was previously omitted, because not all missions (e.g., scientific missions) included this event. Following the Columbia accident in 2003 (which is referred to as return-to-flight), all but one mission has been to the ISS, so now rendezvous and docking is considered part of a nominal mission and included in the SPRA. Failure to rendezvous and dock to the ISS, as it relates to mission success, is not included. Although extravehicular activity occurs within the time period encompassing the SPRA scope; it is excluded from the scope, because it is considered mission-specific.

The SPRA assumes the vehicle configuration is equivalent to that of a generic Orbiter. In keeping with this assumption, hazards associated with payloads are considered mission-specific and are not included the SPRA. The SPRA generally assesses hazards that consist of:

- Equipment functional failures
- Flammable/explosive fluid leaks
- Environment (or external) events, such as MMOD
- Structural failures
- Human errors

Since Shuttle missions vary in payloads, durations, etc., these hazards are assessed in terms of a nominal or "generic" mission, therefore mission specific payloads are not considered. Iteration 3.1 assumes a nominal mission duration of 11.4 days based on an average duration of several selected Shuttle missions. This is slightly longer than the 9 day mission duration that was assessed in Iteration 2.1. The new mission duration is consistent with the mission durations assumed in the MMOD calculation, but is slightly less than the average mission duration of 13.6 days since return-to-flight. The mission is broken into three phases: ascent, orbit, and entry. Success of each phase is dependent on the success of the previous phase.

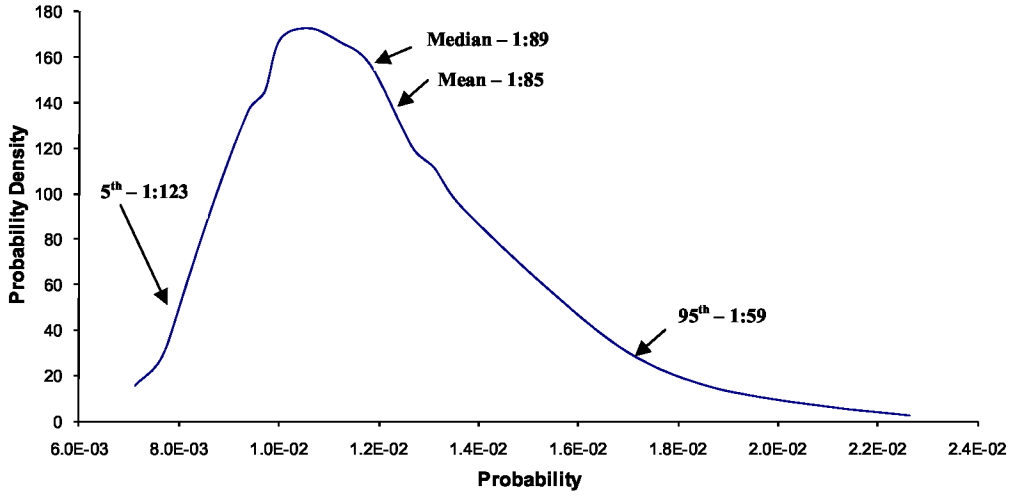
The SPRA generally follows PRA best practices as outlined in the *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners* [2]. However, these practices were augmented based on the uniqueness of the Space Shuttle systems, its operations, and recommendations made by SPRA independent peer reviewers.

While SPRA management resides with SSP Safety & Mission Assurance (S&MA) Office and its technical leadership with the JSC S&MA Directorate, this assessment includes representatives from a variety of organizations. Almost 200 engineers, astronauts, instructors, analysts, and managers have contributed to the SPRA to date. The SPRA methodology was peer reviewed by an independent panel of PRA experts outside NASA. Additionally, the SPRA model logic and failure data were reviewed by each of the project offices within the SSP and the NASA Engineering and Safety Council reviewed specific topics.

3. RESULTS

The mean calculated risk of LOCV during a nominal mission for Iteration 3.1 is 1.2E-02 per mission or 1 in 85 missions with uncertainties of 1 in 59 and 1 in 123 per mission, representing the 95th and 5th percentiles respectively. The actual loss of 2 vehicles over the first 129 Shuttle missions produces a probability of 1 in 65, which is consistent with the calculated results. Figure 1 provides a graphical representation of the calculated results for Iteration 3.1. The corresponding figure for Iteration 2.1 was not presented in PSAM 8; however, the mean was calculated to be 1 in 67 with a 95th percentile of 1 in 45 and a 5th percentile of 1 in 100. Comparing the mean LOCV risk estimate for Iteration 2.1, 1 in 67, as well as the uncertainty with Iteration 3.1 indicates there has been a decrease in risk. This decrease in risk is mainly due to return-to-flight improvements.

Figure 1: Overall Iteration 3.1 Shuttle PRA Uncertainty Distribution



As noted in the PSAM 8 paper [1], the Shuttle mission is dynamic and a failure in one phase (e.g., ascent) may not result in LOCV until a later phase (e.g., entry). Therefore, it is useful to differentiate between when LOCV failures are initiated and when they are realized. Table 1 shows the SPRA Iteration 2.1 overall results when LOCV is initiated and when it is realized. Almost 90% of the estimated risk is initiated on ascent or orbit; however, over two-thirds of the risk is actually realized on entry. For those risks that do not immediately result in LOCV, evaluations may be performed to determine if any potential recovery actions can be taken (e.g., on-orbit tile repair). Table 2 shows that Iteration 3.1 has a similar trend; but since recovery measures such as TPS repair and crew rescue are taken into consideration, the trend is not as pronounced. There is a noticeable increase in the orbit realized risk from 1 in 909 in Iteration 2.1 to 1 in 492 in Iteration 3.1. The incorporation of recovery measures on-orbit also results in a decrease of the entry realized risk from ~1 in 100 to ~1 in 159.

Table 1: SPRA Iteration 2.1 Estimated Phase Contributions to When LOCV is Initiated and When it is Realized [1]

	Estimated Phase Contributions to When LOCV is Initiated		Estimated Phase Contributions to When LOCV is Realized	
Phase	**Per Mission LOCV Probability**	**Percent**	**Per Mission LOCV Probability**	**Percent***
Ascent	1 in 122	54%	1 in 270	25%
Orbit	1 in 208	32%	1 in 909	7%
Entry	1 in 483	14%	1 in 100	68%

Table 2: SPRA Iteration 3.1 Estimated Phase Contributions to When LOCV is Initiated and When it is Realized

	Estimated Phase Contributions to When LOCV is Initiated		Estimated Phase Contributions to When LOCV is Realized	
Phase	**Per Mission LOCV Probability**	**Percent**	**Per Mission LOCV Probability**	**Percent**
Ascent	1 in 207	41%	1 in 288	29%
Orbit	1 in 187	45%	1 in 492	17%
Entry	1 in 600	14%	1 in 159	53%

Another way to summarize these results is a breakdown by element or risk contributor. The Space Shuttle is divided into several major elements: the Orbiter, Space Shuttle Main Engines (SSME), Solid Rocket Boosters (SRB), Reusable Solid Rocket Motors (RSRM), and External Tank (ET). Ascent debris, MMOD, and human error are specifically broken out due to their relatively large contributions. Figure 2 shows the top risk contributors arranged in descending order for Iteration 2.1. Figure 3 shows the same breakdown for Iteration 3.1. Although each basic event is assigned to one or more elements or contributors, some of the risk contributors are broader integration issues (e.g., ascent debris strikes). Comparing the two figures shows that MMOD has moved to be the highest risk contributor. Ascent debris has moved from the top contributor in Iteration 2.1 down to the fifth largest contributor in Iteration 3.1.

Figure 2. SPRA Iteration 2.1 Shuttle LOCV Risk Contributors

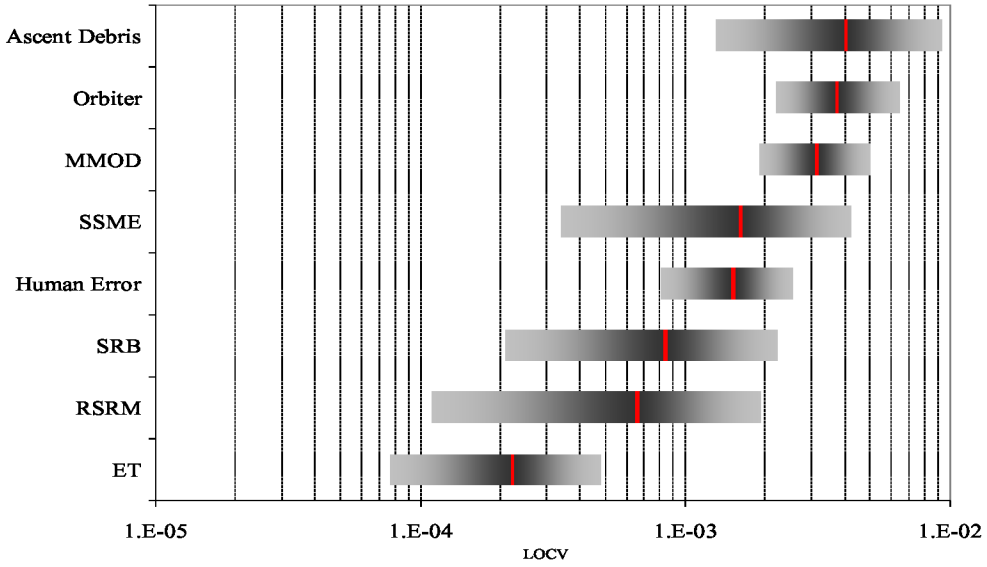
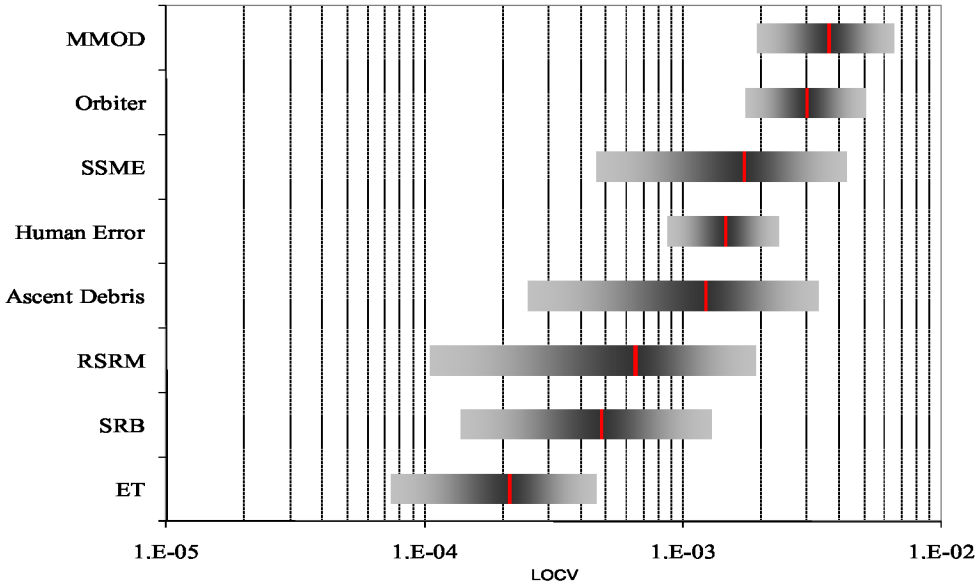


Figure 3. SPRA Iteration 3.1 Shuttle LOCV Risk Contributors



A direct comparison of the top risk rankings and mean probabilities for Iterations 2.1 and 3.1 is provided in Table 3. It is important to note that additional granularity has been added to the risk contributors in Table 3, so there is not a direct correlation to the results provided in Figures 2 and 3. Each scenario in the table may be made up of one or more model cutsets that have the same or similar initiating events and consequences. The top 10 scenarios alone currently represent about ~74% of the total mission risk within the defined SPRA model scope for Iteration 3.1.

Table 3: Dominant LOCV Scenarios

Iteration 3.1 Results				Failure Group	Iteration 2.1 Results	
Rank	% of Total	Cumulative %	Probability (1/n)		Rank	Probability
1	30.9	30.9	3.6E-03 (1 in 277)	MMOD strikes Orbiter on orbit leading to LOCV on orbit or entry	2	3.1E-03 (1 in 320)
2	13.2	44.1	1.5E-03 (1 in 652)	SSME-induced SSME catastrophic failure	3	1.5E-03 (1 in 670)
3	10.2	54.3	1.2E-03 (1 in 840)	Ascent debris strikes Orbiter TPS leading to LOCV on orbit or entry	1	4.0E-03 (1 in 250)
4	7.0	61.3	8.2E-04 (1 in 1,220)	Crew error during entry	4	1.1E-03 (1 in 910)
5	5.6	66.9	6.5E-04 (1 in 1,530)	RSRM-induced RSRM catastrophic failure	5	6.5E-04 (1 in 1,530)
6	1.6	68.5	1.8E-04 (1 in 5,510)	Common cause failure of the Electrical Power System (EPS) on orbit	12	1.8E-04 (1 in 5,510)
7	1.5	70.0	1.7E-04 (1 in 5,890)	SRB Auxiliary Power Unit (APU) shaft seal fracture	8	3.2E-04 (1 in 3,150)
8	1.3	71.3	1.5E-04 (1 in 6,480)	SRB booster separation motor debris strikes Orbiter windows	14	1.5E-04 (1 in 6,480)
9	1.3	72.6	1.5E-04 (1 in 6,640)	An existing crack in the Orbiter APU turbine wheel propagates, resulting in catastrophic failure of the APU during entry	-	-
10	1.2	73.8	1.4E-04 (1 in 7,350)	Common cause failure of the APU System on entry	24	7.6E-05 (1 in 13,000)

In Table 3, the MMOD risk for Iteration 3.1 is roughly the same as Iteration 2.1; however, there have been changes in the success criteria associated with critical damage that would have greatly increased the risk. Specifically, following the Columbia accident, a re-evaluation of ascent debris and MMOD impact damage capability on the Reinforced Carbon-Carbon (RCC) panels, which make up the Orbiter Wing Leading Edge (WLE), would have approximately doubled the risk. However, the incorporation of inspection/repair and crew rescue serves to mitigate the MMOD risk.

Ascent debris is the third-ranked risk contributor, because the Orbiter and human error contributors were broken down into more detailed or specific contributors. Ascent debris was reduced by about 70% (4.0E-03 to 1.2E-03). The reduction is equally attributable to mitigations to minimize ET foam loss as well as on-orbit inspection/repair and crew rescue.

Crew error during entry risk has decreased slightly due to a Bayesian updating of the Cognitive Reliability and Error Analysis Method (CREAM)-calculated values [3] with landing and simulator data.

Crediting a re-design of the SRB shaft seals resulted in a decrease in risk from 3.2E-02 to 1.7E-04; although, the rank moved from #8 to #7 on the top 10 risks.

One scenario on the Iteration 3.1 top 10 contributors was not previously ranked in Iteration 2.1, "An existing crack in the Orbiter APU turbine wheel propagates, resulting in catastrophic failure of the APU during entry." During the data re-evaluation, which was part of the SPRA major update, the failure probabilities associated with the events included in this scenario were determined to be unsubstantiated and new defendable values were used in Iteration 3.1. However, the current estimates

are conservative, because they do not consider inspections put in place to detect surface flaws that could propagate to critical length cracks. The inclusion of this mitigation in the next SPRA iteration will most likely cause this scenario to drop off of the top risk list.

The estimated risk associated with common cause failure of the APUs has roughly doubled (7.6E-05 to 1.4E-04) due to the re-evaluation of the generic prior and Bayesian updating with Shuttle-specific failures.

There are four scenarios that have dropped from the top 10 risks. External leakage in the APUs on entry has fallen from #6 to #15 due to the re-evaluation of the Space Transportation System (STS)-9 APU fire events and model corrections. TPS debond has fallen from #7 to #30 due to the capability to repair or rescue the crew. Reaction Control System failures leading to a center of gravity concern on entry has dropped from the list due to crediting on-orbit mitigations such as providing ballast. The risk of four SRB hold-down bolts hanging up during launch has dropped from the top 10 list, because a structural analysis was completed that showed hang up of four bolts has a low probability of resulting in LOCV.

4. CONCLUSION

The SPRA is currently the most comprehensive and peer-reviewed NASA PRA. As with any PRA of a large, complex, and engineered system, the SPRA is developed for a defined scope; and engineering judgment is used to make assumptions where necessary. Therefore, limitations exist as to its use. However, the SPRA is only one part of the risk-informed decision-making process. Operational constraints, qualitative risk assessments, budgetary considerations, etc., are also integral parts of the program decision-making process. The following are primary limitations and observations regarding the current SPRA scope.

- Does not include mission-specific on-orbit operations (e.g., extravehicular activity).
- Does not include all flight rules, and therefore all pre-planned operational procedures.
- Does not encompass ground operations (e.g., tanking, scrub turnaround, ground tracking, crew egress, etc.). Note that in some cases, ground-induced failures are incorporated in defined failure rate functions. However, ground processing is not explicitly modeled.

The Shuttle is a very reliable vehicle in comparison with other launch systems. Much of the risk posed by Shuttle operations is related to fundamental aspects of the spacecraft design and the environments in which it operates. Since the SSP is nearing its end, it is unlikely that design improvements can be implemented to address these risks prior to retirement. However, the SPRA indicates there are areas that offer potential for improvement, for example, in the areas of: MMOD, ascent debris, ground and flight crew training, and operational flexibility.

The SPRA is intended to be used as a risk management tool. The SPRA provides insights into the significant risks of Space Shuttle flight. The SPRA model results produced the following insights:

- The calculated overall mean estimate for LOCV highly agrees with flight history. As described earlier, the historical LOCV probability is 1 in 65, which corresponds well with the SPRA risk estimate of 1 in 85. The decrease over the previously reported probability, 1 in 67, is mainly due to return-to-flight improvements, which were not reflected in the previous model.
- An estimated 82% of Shuttle LOCV calculated risk is realized during ascent and entry. This estimation represents a small fraction of overall mission duration and may be the result of the current ground rule to not include mission-specific on-orbit activities. Most of the ascent and entry risk is related to the inherent design and operating environment of the Shuttle, and therefore would be difficult to improve without significant design changes. However, the results emphasize the contribution of ascent debris and MMOD to the overall mission risk.

- With consideration given to TPS repair techniques and crew rescue in the model, the risk of LOCV events manifesting during entry has been reduced. However, approximately 40% of the risk is associated with scenarios that are potentially recoverable during orbit if the risk condition is isolated and controlled prior to entry. Therefore, efforts to provide greater operational capability for risk recovery should be further developed. For example, incorporating the Integrated Sensor Inspection System (ISIS) Digital Camera (IDC) into the TPS inspection process improves detection capability and contributes to an overall Orbiter LOCV risk reduction.
- Human errors of commission during the latter stages of entry (e.g., landing exceeds maximum sink rate) contribute to about 7% of the overall mission risk. Since this is an area where risk can easily increase, NASA should maintain appropriate training and procedural practices in the latter stages of entry.

Acknowledgements

The authors would like to thank the SSP for supporting this analysis as well as the engineers, astronauts, instructors, analysts, and managers that have contributed to the SPRA to date.

References

[1] Boyer, R.L. et al., "Space Shuttle Probabilistic Risk Assessment Overview" PSAM 8, New Orleans, Louisiana, May 2006.

[2] Stamatelatos M. et al., *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, Version 1.1, NASA Office of Safety and Mission Assurance, NASA Headquarters, Washington, D.C., 2002.

[3] Hollnagel, E., "*Cognitive Reliability and Error Analysis Method—CREAM*", Elsevier Science, Oxford, 1998.

2009 SPACE SHUTTLE PROBABILISTIC RISK ASSESSMENT OVERVIEW

Teri L. Hamlin[a], Michael A. Canga[a], Roger L. Boyer[a], and Eric B. Thigpen[b]

[a]National Aeronautics and Space Administration (NASA), Houston, USA

[b]Science Applications International Corporation (SAIC), Houston, USA

INTRODUCTION

- National Aeronautics and Space Administration (NASA) initially used Failure Modes and Effects Analysis as well as Hazard Analysis to understand the risks associated with Space Shuttle flight.
  - However, the qualitative nature of these assessments can lead to inconsistency and imprecision in risk characterization that make risk prioritization difficult and risk aggregation impossible.
- The SPRA was initiated to provide a useful risk management tool for identifying strengths and possible weaknesses in the Shuttle design and operation.
  - Mostly typical PRA model in that it is based on fault trees and event trees populated with failure rate and probability data. However, it is unique because of the dynamic nature of the mission and environment it models.
  - SPRA is a living analysis. The latest revision to the SPRA is Iteration 3.1, and it will not be the last as additional risk insight is gained about the Shuttle and used to support subsequent Shuttle flights.
- This presentation provides the SPRA Iteration 3.1 analysis and results and compares them to those previously presented in 2006 as SPRA Iteration 2.1.
- The SPRA has undergone two minor revisions and one major revision since PSAM 8.
  - The minor updates included the addition of on-orbit inspection/repair and crew rescue.
  - Other minor updates also corrected errors detected in the previous version of the SPRA model.
  - The major update expanded the SPRA scope to include benign engine shutdown and stuck throttle aborts during ascent as well as rendezvous and docking operations in orbit.
    - Including aborts significantly increased the complexity of the SPRA model but the added risk was minimal, less than 1%.
  - The major SPRA update also included a reevaluation of the data.

SCOPE

- The SPRA includes hazards that may result in an in-flight Loss of Crew and Vehicle (LOCV)
  - In-flight is defined as the time from liftoff (T-0) to wheel stop.
- Iteration 3.1 has expanded the scope of a "nominal" mission, as compared to Iteration 2.1, to include rendezvous and docking with the ISS as well as ascent aborts.
  - Rendezvous and docking was previously omitted, because not all missions (e.g., scientific missions) included this event. Following the Columbia accident in 2003 (which is referred to as return-to-flight), all but one mission has been to the ISS, so now rendezvous and docking is considered part of a nominal mission and included in the SPRA.
- Failure to rendezvous and dock to the ISS, as it relates to mission success, is not included.
- Although extravehicular activity occurs within the time period encompassing the SPRA scope; it is excluded from the scope, because it is considered mission-specific.
- The SPRA assumes the vehicle configuration is equivalent to that of a generic Orbiter with a generic mission.
  - Hazards associated with payloads are considered mission-specific and are not included the SPRA.
  - Iteration 3.1 assumes a nominal mission duration of 11.4 days based on an average duration of several selected Shuttle missions.
    - This is slightly longer than the 9 day mission duration that was assessed in Iteration 2.1.
    - The new mission duration is consistent with the mission durations assumed in the MMOD calculation, but is slightly less than the average mission duration of 13.6 days since return-to-flight.
  - The mission is broken into three phases: ascent, orbit, and entry. Success of each phase is dependent on the success of the previous phase.

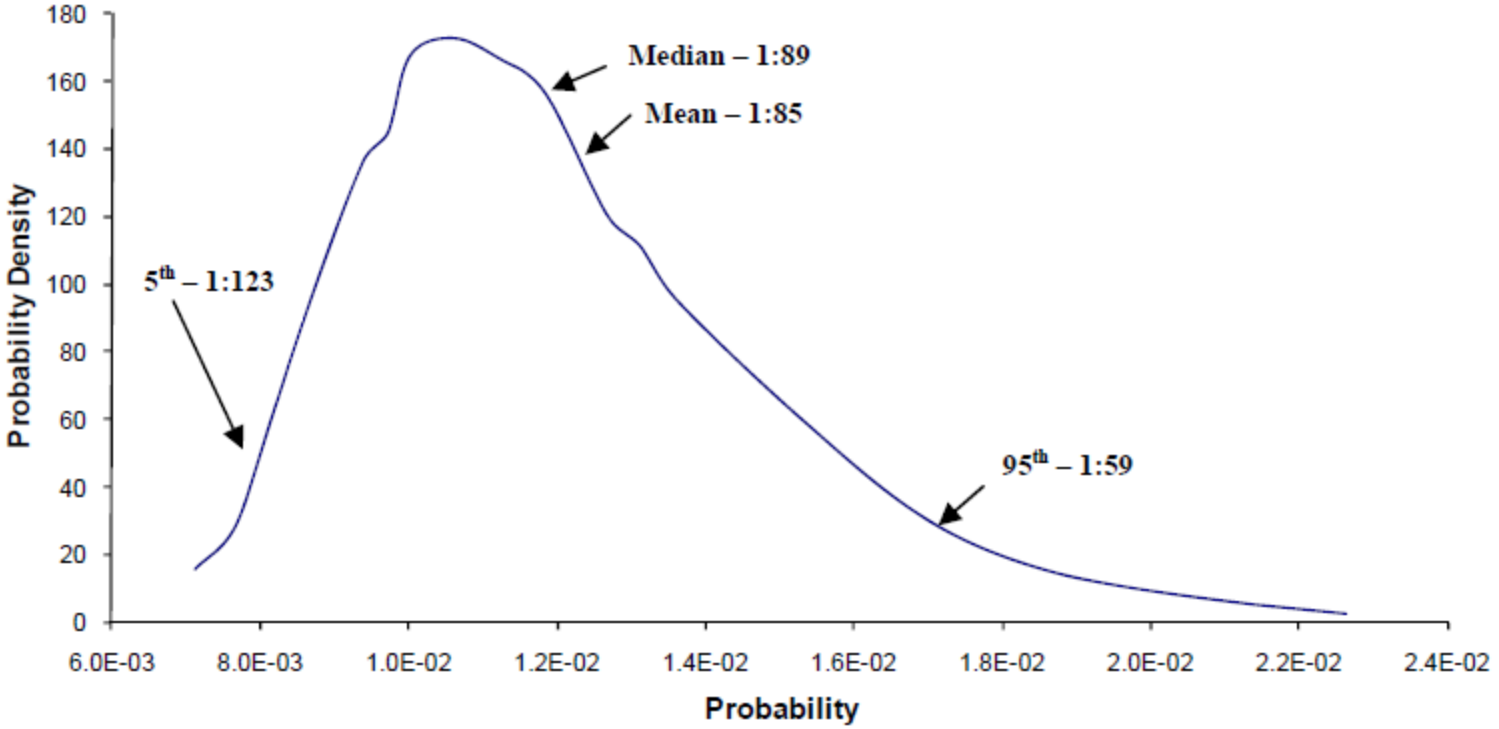
METHODOLOGY

- The SPRA generally follows PRA best practices as outlined in the Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners. However, these practices were augmented based on the uniqueness of the Space Shuttle systems, its operations, and recommendations made by SPRA independent peer reviewers.
- The SPRA generally assesses hazards that consist of:
  - Equipment functional failures
  - Flammable/explosive fluid leaks
  - Environment (or external) events, such as MMOD
  - Structural failures
  - Human errors

SPRA TEAM

- While SPRA management resides with SSP Safety & Mission Assurance (S&MA) Office and its technical leadership with the JSC S&MA Directorate, this assessment includes representatives from a variety of organizations.
- Almost 200 engineers, astronauts, instructors, analysts, and managers have contributed to the SPRA to date.
- The SPRA methodology was peer reviewed by an independent panel of PRA experts outside NASA.
- Additionally, the SPRA model logic and failure data were reviewed by each of the project offices within the SSP and the NASA Engineering and Safety Council reviewed specific topics.

OVERALL ITERATION 3.1 SHUTTLE PRA UNCERTAINTY DISTRIBUTION



- The actual loss of 2 vehicles over the first 129 Shuttle missions produces a probability of 1 in 65, which is consistent with the calculated results.
- The corresponding figure for **Iteration 2.1** was not presented in PSAM 8; however, the mean was calculated to be **1 in 67** with a 95th percentile of **1 in 45** and a 5th percentile of **1 in 100**.
- Comparing the mean LOCV risk estimate for Iteration 2.1, 1 in 67, as well as the uncertainty with Iteration 3.1 indicates there has been a decrease in risk. This decrease in risk is mainly due to return-to-flight improvements.

ESTIMATED PHASE CONTRIBUTIONS TO WHEN LOCV IS INITIATED AND WHEN IT IS REALIZED

SPRA Iteration 2.1

	Estimated Phase Contributions to When LOCV is Initiated		Estimated Phase Contributions to When LOCV is Realized	
Phase	Per Mission LOCV Probability	Percent	Per Mission LOCV Probability	Percent*
Ascent	1 in 122	54%	1 in 270	25%
Orbit	1 in 208	32%	1 in 909	7%
Entry	1 in 483	14%	1 in 100	68%

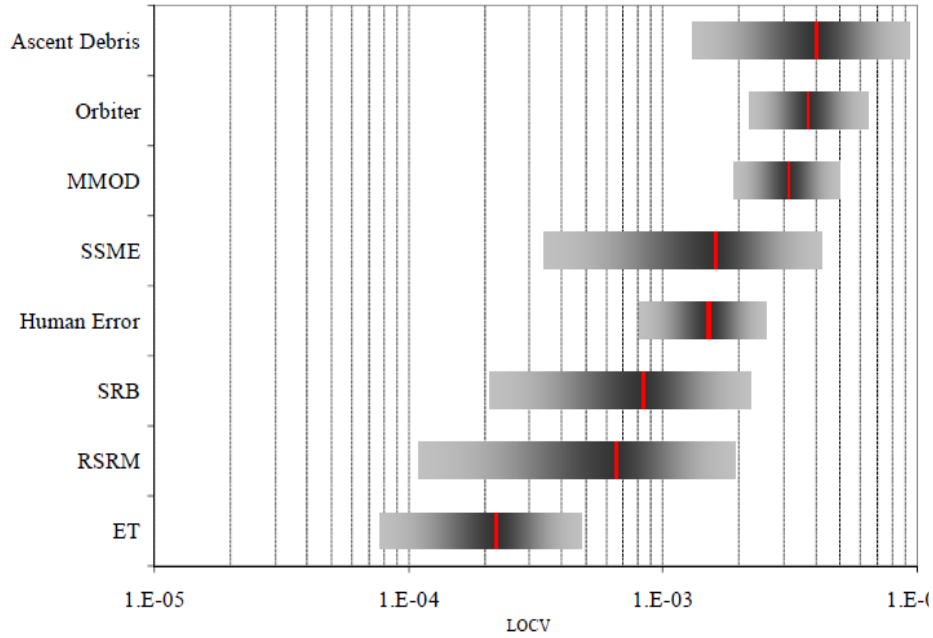
SPRA Iteration 3.1

	Estimated Phase Contributions to When LOCV is Initiated		Estimated Phase Contributions to When LOCV is Realized	
Phase	Per Mission LOCV Probability	Percent	Per Mission LOCV Probability	Percent
Ascent	1 in 207	41%	1 in 288	29%
Orbit	1 in 187	45%	1 in 492	17%
Entry	1 in 600	14%	1 in 159	53%

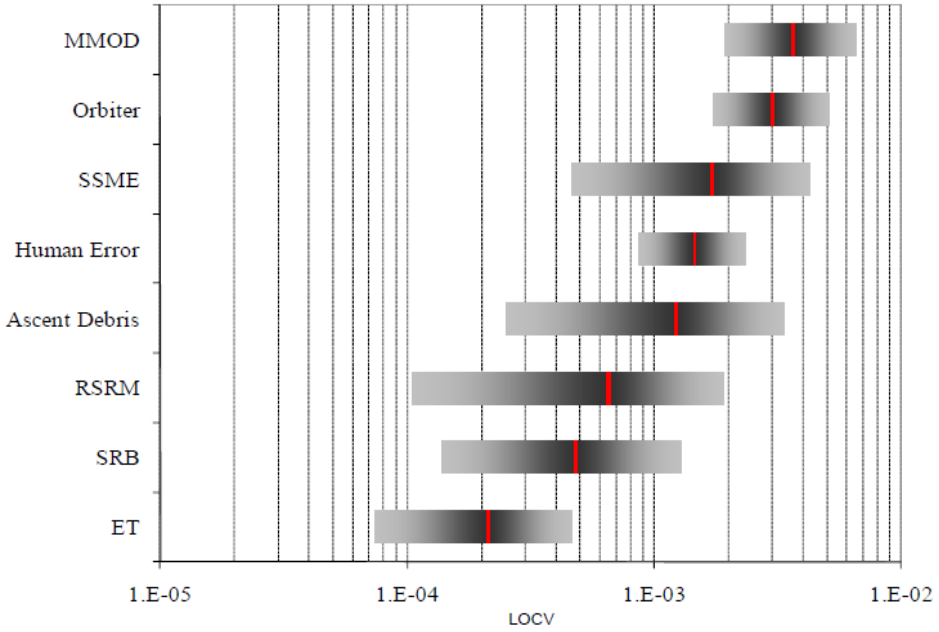
- Shuttle mission is dynamic and a failure in one phase (e.g., ascent) may not result in LOCV until a later phase (e.g., entry).
  - Therefore, it is useful to differentiate between when LOCV failures are initiated and when they are realized.
- For iteration 2.1 almost 90% of the estimated risk is initiated on ascent or orbit; however, over two-thirds of the risk is actually realized on entry.
  - For those risks that do not immediately result in LOCV, evaluations may be performed to determine if any potential recovery actions can be taken (e.g., on-orbit tile repair).
- Iteration 3.1 has a similar trend; but since recovery measures such as TPS repair and crew rescue are taken into consideration, the trend is not as pronounced.
- There is a noticeable increase in the orbit realized risk from 1 in 909 in Iteration 2.1 to 1 in 492 in Iteration 3.1.
- Recovery measures on-orbit also results in a decrease of the entry realized risk from ~1 in 100 to ~1 in 159.

SHUTTLE LOCV RISK CONTRIBUTORS

SPRA Iteration 2.1



SPRA Iteration 3.1



- The Space Shuttle is divided into several major elements
  - Orbiter
  - Space Shuttle Main Engines (SSME)
  - Solid Rocket Boosters (SRB),
  - Reusable Solid Rocket Motors (RSRM)
  - External Tank (ET).
- Ascent debris, MMOD, and human error are specifically broken out due to their relatively large contributions.
- Comparing the two figures shows that MMOD has moved to be the highest risk contributor. Ascent debris has moved from the top contributor in Iteration 2.1 down to the fifth largest contributor in Iteration 3.1.

DOMINANT SPRA LOCV SCENARIOS

Iteration 3.1 Results				Failure Group	Iteration 2.1 Results	
Rank	% of Total	Cumulative %	Probability (1/n)		Rank	Probability
1	30.9	30.9	3.6E-03 (1 in 277)	MMOD strikes Orbiter on orbit leading to LOCV on orbit or entry	2	3.1E-03 (1 in 320)
2	13.2	44.1	1.5E-03 (1 in 652)	SSME-induced SSME catastrophic failure	3	1.5E-03 (1 in 670)
3	10.2	54.3	1.2E-03 (1 in 840)	Ascent debris strikes Orbiter TPS leading to LOCV on orbit or entry	1	4.0E-03 (1 in 250)
4	7.0	61.3	8.2E-04 (1 in 1,220)	Crew error during entry	4	1.1E-03 (1 in 910)
5	5.6	66.9	6.5E-04 (1 in 1,530)	RSRM-induced RSRM catastrophic failure	5	6.5E-04 (1 in 1,530)
6	1.6	68.5	1.8E-04 (1 in 5,510)	Common cause failure of the Electrical Power System (EPS) on orbit	12	1.8E-04 (1 in 5,510)
7	1.5	70.0	1.7E-04 (1 in 5,890)	SRB Auxiliary Power Unit (APU) shaft seal fracture	8	3.2E-04 (1 in 3,150)
8	1.3	71.3	1.5E-04 (1 in 6,480)	SRB booster separation motor debris strikes Orbiter windows	14	1.5E-04 (1 in 6,480)
9	1.3	72.6	1.5E-04 (1 in 6,640)	An existing crack in the Orbiter APU turbine wheel propagates, resulting in catastrophic failure of the APU during entry	-	-
10	1.2	73.8	1.4E-04 (1 in 7,350)	Common cause failure of the APU System on entry	24	7.6E-05 (1 in 13,000)

COMPARISON OF DOMINANT SPRA LOCV SCENARIOS

- MMOD is roughly the same but it is a coincidence. Damage criteria was revised post Columbia which increased the probability of critical damage but inspection with Repair and Crew Rescue mitigated the increased risk
- Ascent debris was reduced by about 70% (4.0E-03 to 1.2E-03) due to mitigations to minimize ET foam loss as well as on-orbit inspection / repair and crew rescue
- Crew error during entry risk has decreased slightly due to a Bayesian updating with landing and simulator data.
- Crediting a re-design of the SRB shaft seals in a decrease in risk from resulted 3.2E-04* to 1.7E-04; although, the rank moved from #8 to #7 on the top 10 risks.
- #9 on top 10 contributors was not previously ranked in Iteration 2.1. The failure probabilities associated with the events included in this scenario were determined to be unsubstantiated and new defendable values were used in Iteration 3.1.
  - However, the current estimates are conservative, because they do not consider inspections put in place to detect surface flaws that could propagate to critical length cracks. The inclusion of this mitigation in the next SPRA iteration will most likely cause this scenario to drop off of the top risk list.

*** In the paper this value was reported at 3.2E-02 which is a typo**

COMPARISON OF DOMINANT SPRA LOCV SCENARIOS (2)

- The estimated risk associated with common cause failure of the APUs has roughly doubled (7.6E-05 to 1.4E-04) due to the re-evaluation of the generic prior and Bayesian updating with Shuttle-specific failures.
- There are four scenarios that have dropped from the top 10 risks.
  - External leakage in the APUs on entry has fallen from #6 to #15 due to the re-evaluation of the Space Transportation System (STS)-9 APU fire events and model corrections.
  - TPS debond has fallen from #7 to #30 due to the capability to repair or rescue the crew.
  - Reaction Control System failures leading to a center of gravity concern on entry has dropped from the list due to crediting on-orbit mitigations such as providing ballast.
  - The risk of four SRB hold-down bolts hanging up during launch has dropped from the top 10 list, because a structural analysis was completed that showed hang up of four bolts has a low probability of resulting in LOCV.

CONCLUSION: LIMITATIONS

- The SPRA is currently the most comprehensive and peer-reviewed NASA PRA. As with any PRA of a large, complex, and engineered system, the SPRA is developed for a defined scope; and engineering judgment is used to make assumptions where necessary. The following are primary limitations and observations regarding the current SPRA scope.
  - Does not include mission-specific on-orbit operations (e.g., extravehicular activity).
  - Does not include all flight rules, and therefore all pre-planned operational procedures.
  - Does not encompass ground operations (e.g., tanking, scrub turnaround, ground tracking, crew egress, etc.). Note that in some cases, ground-induced failures are incorporated in defined failure rate functions. However, ground processing is not explicitly modeled.
- The Shuttle is a very reliable vehicle in comparison with other launch systems.
  - Much of the risk posed by Shuttle operations is related to fundamental aspects of the spacecraft design and the environments in which it operates.
- Since the SSP is nearing its end, it is unlikely that design improvements can be implemented to address these risks prior to retirement. However, the SPRA indicates there are areas that offer potential for improvement, for example, in the areas of: MMOD, ascent debris, ground and flight crew training, and operational flexibility.

CONCLUSION: INSIGHTS

- The SPRA is intended to be used as a risk management tool and provides insights into the significant risks of Space Shuttle flight. The SPRA model results produced the following insights:
  - The calculated overall mean estimate for LOCV highly agrees with flight history.
    - historical LOCV probability is 1 in 65, which corresponds well with the SPRA risk estimate of 1 in 85. The decrease over the previously reported probability, 1 in 67, is mainly due to return-to-flight improvements, which were not reflected in the previous model.
  - An estimated 82% of Shuttle LOCV calculated risk is realized during ascent and entry.
    - A small fraction of overall mission duration and may be the result of the current ground rule to not include mission-specific on-orbit activities.
    - Most of the ascent and entry risk is related to the inherent design and operating environment of the Shuttle, and therefore would be difficult to improve without significant design changes.
    - Results emphasize the contribution of ascent debris and MMOD to the overall mission risk.
  - With consideration given to TPS repair techniques and crew rescue in the model, the risk of LOCV events manifesting during entry has been reduced. However, approximately 40% of the risk is associated with scenarios that are potentially recoverable during orbit if the risk condition is isolated and controlled prior to entry.
    - Therefore, efforts to provide greater operational capability for risk recovery should be further developed. For example, incorporating the Integrated Sensor Inspection System (ISIS) Digital Camera (IDC) into the TPS inspection process improves detection capability and contributes to an overall Orbiter LOCV risk reduction.
  - Human errors of commission during the latter stages of entry (e.g., landing exceeds maximum sink rate) contribute to about 7% of the overall mission risk.
    - Since this is an area where risk can easily increase, NASA should maintain appropriate training and procedural practices in the latter stages of entry.