View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by NASA Technical Reports Server

DYNAMIC SIMULATION PROBABALISTIC RISK ASSESSMENT MODEL FOR AN ENCELADUS SAMPLE RETURN MISSION

Christopher J. Mattenberger[a], Donovan L. Mathias[b], and Ken Gee[c]

[a]*STC, NASA Ames Research Center, M/S 258-6, Moffett Field, CA, 94305, chris.mattenberger@nasa.gov*
[b]*NASA Ames Research Center, M/S 258-5, Moffett Field, CA, 94305, donovan.mathias@nasa.gov*
[c]*NASA Ames Research Center, M/S 258-1, Moffett Field, CA, 94305, ken.gee-1@nasa.gov*

Enceladus, a moon of Saturn, has geyser-like jets that spray plumes of material into orbit. These jets could enable a free-flying spacecraft to collect samples and return them to Earth for study to determine if they contain the building blocks of life. The Office of Planetary Protection at NASA requires containment of any unsterilized samples and prohibits destructive impact of the spacecraft upon return to Earth, with a sample release probability of less than 1 in 1,000,000 as a recommended goal.

This paper describes a probabilistic risk assessment model that uses dynamic simulation techniques to capture the physics-based, time- and state-dependent interactions between the sample return system and the environment, which drive the risk of sample release. The dynamic approach uses a Monte Carlo-style simulation to integrate the many phases and sources of risk for a sample return mission.

The model is used to assess the achievability of the planetary protection reliability goal. This is accomplished by performing sensitivity studies assessing the impact of modeling assumptions to identify where uncertainties drive the risk. These results, in turn, are used to examine the feasibility of meeting key design and performance parameters that are needed to achieve the reliability goal for a given architecture with existing technologies.

I. INTRODUCTION

Discovering a second genesis of life outside of Earth's biosphere would have profound impacts on our understanding of biology and our place in the universe. Within the solar system, there are multiple locations that may have once had or may still harbor life. One potential location is Enceladus, the sixth largest moon of Saturn. Enceladus is a prime candidate to support life as it shows evidence of internal heat and a large ocean beneath an icy shell. In 2005, the Cassini spacecraft discovered that Enceladus has geyser-like jets spraying into orbit around Saturn, making up the E ring. The jets contain water, CO_2, CO, CH_4, NH_3, and Ar, as well as evidence of other more complex organic molecules[1]. These geysers could enable a free-flying spacecraft to collect samples of compounds found on Enceladus without needing to land on the surface, greatly simplifying the equipment required to return samples to Earth for study.

Returning samples to Earth for study allows independent and repeatable studies to be performed by multiple scientists with varying techniques and instruments, many of which would be impractical in space. Furthermore, sample studies performed on Earth can take advantage of the latest state-of-the-art techniques available, and new techniques can be developed and applied based upon preliminary results[2].

The Office of Planetary Protection (OPP) at the National Aeronautics and Space Administration (NASA) is responsible for ensuring that space missions take prudent precautions to protect Earth's biosphere from biological threats that may exist in samples brought back from space. The OPP prohibits destructive impact upon return of a spacecraft and requires highly reliable containment of unsterilized samples. This requirement has been interpreted to state that the chance of releasing an unsterilized sample into Earth's biosphere on a reentry attempt should be less than 1 in 1,000,000 (Ref. 3).

Despite the lack of an existing Enceladus Sample Return Mission (ESRM), the achievability of this ambitious planetary protection reliability goal is studied through analysis of a representative architecture. This study seeks to identify key assumptions and uncertainties that drive risk, while determining design and performance parameters necessary to achieve the planetary protection reliability goal. A Monte Carlo-style probabilistic risk assessment (PRA) model has been created using dynamic simulation techniques to capture the physics-based, time- and state-dependent interactions between the sample return system and the environment.

While many phases of an ESRM could be modeled with more traditional, static PRA approaches, a simulation approach greatly facilitates the modeling of the highly dynamic entry, descent, and landing (EDL) phase, when the potential for sample release is most critical. A simulation approach is advantageous because it naturally and accurately accounts for the highly coupled stochastic characteristics of the environment, the performance of the system in a potentially degraded state, and the complex

temporal interactions involved—all of which can dramatically alter the eventual outcome of the mission.

In previous study of the feasibility of a Mars Sample Return (MSR) architecture, an ambitious set of reliability goals for Earth Entry Vehicle (EEV) functionality were proposed. The goals, if met, would ostensibly assure that the risk of Loss of Containment Assurance (LOCA) of unsterilized samples would meet the planetary protection reliability goal[4]. This present ESRM risk study expands upon the previous MSR efforts and examines the achievability of its proposed reliability goals in order to produce a preliminary risk scoping assessment of the ESRM concept. To accomplish this, we developed a model framework that can capture the dependencies between the risk of loss of mission (LOM) and the risk of LOCA, which is a subset of LOM.

II. ENCELADUS SAMPLE RETURN MISSION

As there is currently no complete ESRM architecture available and the design details needed to build a PRA model are absent, this paper focuses on the development of the risk assessment approach that will support the design, development, testing, and evaluation of potential future mission concepts. However, multiple, high-level mission architectures have been developed by the Jet Propulsion Laboratory, California Institute of Technology, under contract from NASA[2,5]. In addition, design details from similar phases of an MSR mission[6] have been adopted in the present work. Based upon this previous work, a generic ESRM architecture has been synthesized to begin developing a dynamic PRA model. Figure 1 shows the ESRM phases and durations.

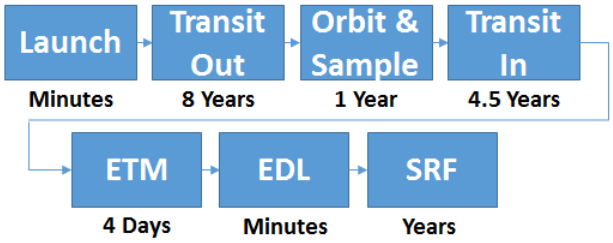

Fig. 1. Major ESRM phases and durations, including Earth targeting maneuver (ETM), entry, descent and landing (EDL) and sample return facility (SRF).

The mission begins with the launch of the probe. The probe consists of an EEV protectively housed within a micrometeoroid and orbital debris (MMOD) shield, along with a main satellite bus that provides command and data handling (C&DH), electrical power system (EPS), propulsion (PROP), communications (COMM), and guidance, navigation and control (GNC). The EEV contains the necessary equipment and mechanisms to collect samples of the geyser plumes and contain them until retrieved by scientists on Earth. Figure 2 shows the axisymmetric geometry adopted for this analysis based upon the MSR EEV[4].

The probe will perform several planetary fly-by maneuvers around Venus, Earth, and Jupiter in order to gain additional energy, and will arrive at Saturn eight years after launch. The probe will then enter Saturn orbit and perform several "pump-down" fly-by maneuvers around Saturn's moons to reduce its energy in a non-propulsive fashion. The spacecraft will spend the next year sampling the geysers of Enceladus and performing other in situ research. To leave Saturn orbit and return to Earth, the spacecraft performs several "pump-up" fly-by maneuvers around several moons in order to gain energy.

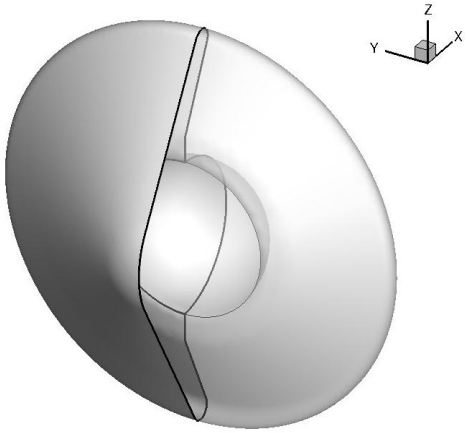

Fig. 2. Axisymmetric EEV geometry.

Approximately four and a half years later, the spacecraft will be prepared to perform the Earth targeting maneuver (ETM). The ETM serves as the final commit-to-return point of the mission. If containment breach is suspected and this maneuver is not completed, then the spacecraft will enter a relatively safe heliocentric orbit to prevent the possible contamination of Earth's biosphere. Once the spacecraft is four days away from Earth, the ETM is performed if the spacecraft bus and EEV have passed final status checks and the MMOD shield has been successfully separated from the spacecraft. The spacecraft bus will use the main engine to place the EEV on a ballistic trajectory to land passively at the Utah Test and Training Range (UTTR). After a successful engine burn, the spacecraft bus will spin-eject the EEV, and then perform a subsequent propulsive burn to place itself in a safe heliocentric orbit.

Given the initial state of the vehicle at separation, the EEV will passively fall to the Earth for the next four days until reaching the entry interface (EI) with the upper atmosphere. During this free-flight, the EEV's now exposed thermal protection system (TPS) will accrue risk from MMOD threats. Absent a specific, detailed ESRM architecture, assumptions about the EEV conditions at EI

have been made based upon existing missions and analyses. Table I shows the assumed nominal mission conditions at EI adopted from the Stardust mission[7] and the MSR mission[4].

TABLE I. EI Conditions.

Parameter	Value
Velocity	16 km/s
Azimuth	102.9 deg
Flight Path Angle	-7.7 deg
Altitude	121.92 km
Longitude	-123.67454 deg
Latitude	42.60499 deg
Mass	39.9 kg

The EEV will then perform EDL, relying on the TPS to protect its structure from the intense heat of atmospheric entry. This heat must effectively sterilize the entire exterior of the EEV[4]. As the EEV is subjected to the dynamic pressure of the atmosphere, the vehicle must maintain integrity, which is sensitive to the temperature of the underlying structure.

Unlike previous sample return missions, the EEV does not rely on a parachute to further decelerate the vehicle. It will impact the UTTR at some final position, which is a function of the initial state at release from the spacecraft bus and the specific interaction with the atmospheric conditions encountered, including winds aloft.

Finally, the EEV is retrieved by the awaiting recovery team and carefully transported to a sample return facility (SRF). The SRF must provide an environment that combines the capabilities of a Bio-Safety Level-4 facility[8] to contain the samples and avoid LOCA, and the capabilities of the Lunar Material Processing Facility, which is designed to prevent LOM due to contamination of the sample with terrestrial matter.

III. RISK MODEL DESCRIPTION

A dynamic risk model is implemented in a Monte Carlo-style framework and follows an approach similar to previous efforts by the Engineering Risk Assessment team at NASA Ames Research Center[9]. This dynamic approach allows for complete system state information to be propagated through the entire mission, from launch to EEV processing at an SRF. The model begins by considering the risk of a launch vehicle failure based upon a generic launch vehicle[10]. Next, the reliabilities of the various spacecraft subsystems are tracked over time, along with the time-varying environmental and MMOD hazards faced by the spacecraft. Prior to arrival at Saturn, any critical loss of spacecraft functionality leads to a LOM.

Once the spacecraft begins collecting samples of the Enceladus geysers, a series of mechanisms must function properly and in situ measurements can begin. Any complete loss of spacecraft functionality at this point in the mission leads to a LOM, in which some in situ science has been performed. Dynamic risk models allow for the exact time LOM occurs to impact the utility produced by the mission.

Until the spacecraft is able to perform the ETM, there is no risk of LOCA. Up until this point in the mission, the modeling approach remains somewhat static, comprised of traditional component reliabilities with the addition of MMOD damage to the probe and the EEV TPS, which can be somewhat dynamic if modeled in detail. It is assumed that the EEV TPS is well protected up to this point by the MMOD shielding provided by the spacecraft bus, and that the ETM would not occur if any damage to the TPS is detected. If the ETM fails to occur or the mission is aborted, the risk of LOCA remains zero and a LOM occurs.

Once the ETM is attempted, there are potential mission end states that could lead to a LOCA, a LOM, or a successful mission. After the ETM is attempted, the phenomena that drive the risk of both LOCA and LOM are now highly time- and state-dependent, physics-based interactions of the system and environment. Once the ETM is complete and EEV separation has occurred, the spacecraft bus performs an additional burn to avoid returning to Earth. Failure of this burn is assumed to result in LOCA.

During the four-day cruise to Earth after the ETM, any significant damage to the TPS could result in LOCA, since the system is then on a passive, ballistic trajectory to the UTTR landing site. To capture this source of risk, an MMOD flux model must be used in conjunction with the cross-sectional area of the EEV. Currently, the risk of MMOD damage to the satellite bus and EEV TPS is based on the MSR analysis[6], which only accounts for catastrophic failures leading to LOM. Thus, the present model assumes that the EEV TPS begins EI in a non-damaged state.

The initial position and velocity of the EEV are propagated to EI using OTIS[11], a trajectory optimization code. OTIS produces a predicted landing point utilizing the 1976 standard atmosphere model[12]. Figure 3 shows the geocentric spherical and vehicle coordinate systems used in OTIS.

For OTIS to propagate the EEV trajectory to the UTTR, estimates for EEV drag as a function of velocity are necessary. These estimates were obtained from computational fluid dynamics analyses, which were performed with CART3D[13] for speeds below Mach 1.2 and with CBAERO[14] for Mach 1.2 and above on the EEV geometry (Figure 2). Figure 4 shows an example of output from CART3D at Mach 0.7.

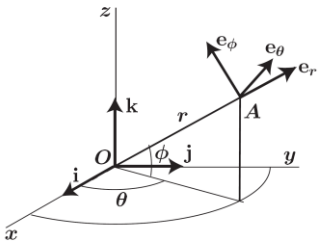

Fig. 3. Spherical coordinate system with the Earth at the origin point O and the EEV point A at ETM.

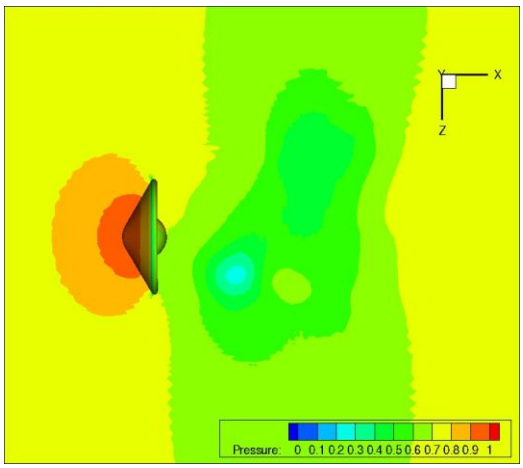

Fig. 4. Example pressure field output from CART3D for Mach = 0.7 and angle of attack = 0 degrees.

In addition to the velocity dependence of supersonic and hypersonic drag, CBAERO is also used to predict the aero-thermodynamic environment on selected body points of the EEV, based on the flow conditions at each OTIS trajectory time step. Figure 5 shows an example of surface heating output from CBAERO for a speed of Mach 45, which is typical of early Earth entry for this mission.

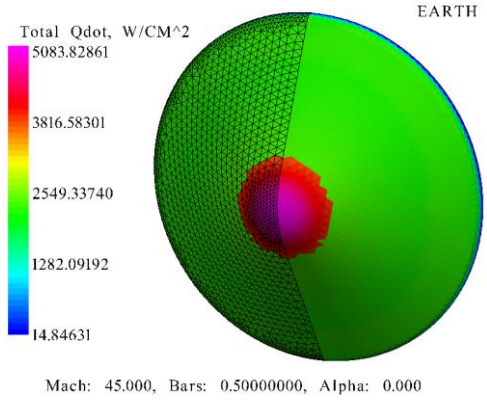

Fig. 5. Example output of convective heating from CBAERO for Mach = 45, angle of attack = 0 degrees, and pressure = 0.5 bars.

The thermal environments produced by CBAERO are then used in a one-dimensional heating code, FIAT[15], to evaluate the response of the EEV TPS. FIAT is used to assess the particular TPS stack-up at the selected body points—i.e., the aerodynamic stagnation point and the point on the back shell that experiences the minimum surface temperature on the vehicle—and produce a time-history of the bondline temperature (BLT) at the interface between the TPS and the spacecraft structure. The stack-up adopted in the present study is identical to that of the MSR design, but with an increased total thickness, consisting of 3.05 cm of carbon phenolic[16,17], which is assumed to be at 233 K at EI. The model does not consider uncertainties in the initial temperature of the EEV TPS. The current model also assumes the TPS will be functionally reliable and does not take into account potential failures modes of this particular TPS stack-up, as they are highly design-specific and are beyond the scope of this study. Figures 6 and 7 show examples of FIAT time-history outputs for the nominal case at the aerodynamic stagnation point on the heat shield, which experiences the greatest surface and bondline temperatures, and at the point on the back shell that experiences the lowest maximum surface temperature.

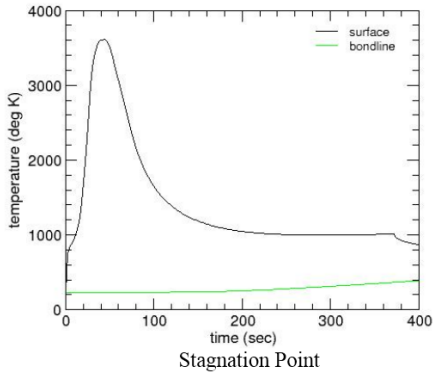

Fig. 6. Example FIAT output of temperature histories at the stagnation point for nominal mission conditions.

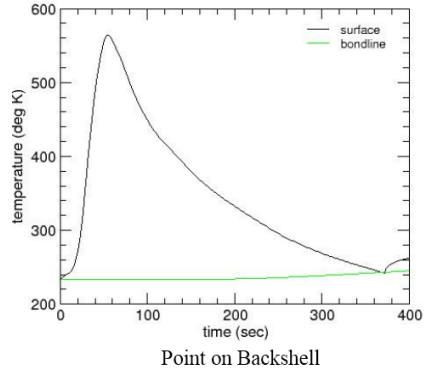

Fig. 7. Example FIAT output of temperature histories on a back-shell point for nominal mission conditions.

To determine the outcome of the mission during the EDL phase in each Monte Carlo realization, outputs from these physics-based simulations are compared to several failure criteria. As an initial assumption in the PRA model, four simple failure criteria have been selected to produce estimates of LOCA probabilities from the physical analysis. Table II shows the baseline failure thresholds that will trigger a LOCA or LOM if violated. The model does not include either the risk of LOCA after a successful landing or the risk of LOM due to the sample being destroyed by excessive heat after landing.

TABLE II. Baseline failure thresholds.

Threshold	Value	Event	Triggers
Sterilization Surface Temperature	398 K - 773 K	Does Not Exceed	LOCA
Structural Failure Temperature at MaxQ	520 K	Exceeds	LOCA
Structural Failure Temperature at Landing	520 K	Exceeds	LOCA
Structural Failure due to Landing Error	84 km	Exceeds	LOCA
Internal Self-Sterilization Temperature	746 K	Exceeds	LOM

The model assumes that the entire exterior surface of the EEV is contaminated during sample collection. Therefore, a LOCA will occur on a particular realization if the lowest of the maximum surface temperatures is not sufficient to sterilize the craft. The sterilization surface temperature value is assumed to be 398 K, based upon planetary protection procedures for the Viking mission[18]. However, as this value does not account for the duration of the temperature exposure, a more stringent procedure requiring 773 K for at least 0.5 seconds is also applied to investigate sensitivity to this parameter[18].

If the maximum BLT at touchdown is above 520 K, then it is assumed that a structural failure occurs on impact and results in a LOCA. Similarly, if the maximum BLT at maximum dynamic pressure (MaxQ) is above 520 K, then it is assumed that aerodynamic forces fail the structure and cause LOCA. This threshold value is based upon the maximum BLT of the MSR design[4].

If the touchdown location is outside of the UTTR region, which is assumed to be 100% soft clay or sand, then the EEV is lost or a structural failure due to landing on a hard surface occurs and results in LOCA. The amount of landing error distance beyond which structural failure occurs is assumed to be 84 km, based upon the Genesis mission[19].

Additionally, the model assumes that the EEV will have an internal self-sterilization functionality to avoid LOCA and instead only cause a LOM. This functionality is passively activated if any portion of the EEV TPS BLT reaches the internal self-sterilization threshold temperature before landing. In such an event, a thermite mixture would be ignited, creating a plasma that would effectively sterilize the sample. The internal self-sterilization threshold value is assumed to be 746 K, which is the auto-ignition temperature of thermite. It is also assumed that if this functionality is activated, then surface sterilization has also occurred.

Finally, the risk associated with transport to the SRF and activities at the SRF must be taken into account. The present model tracks this risk of LOCA as 10^{-7}, which is based upon the MSR analysis[4]. However, it does not consider the risk to individuals working within the SRF or the risk of LOM due to the contained sample becoming contaminated by terrestrial matter.

The possible end states of the model are summarized in the diagram shown in Figure 8. The diagram highlights the interplay between the risk of LOCA, the risk of LOM, and mission success based upon key design and performance parameters.

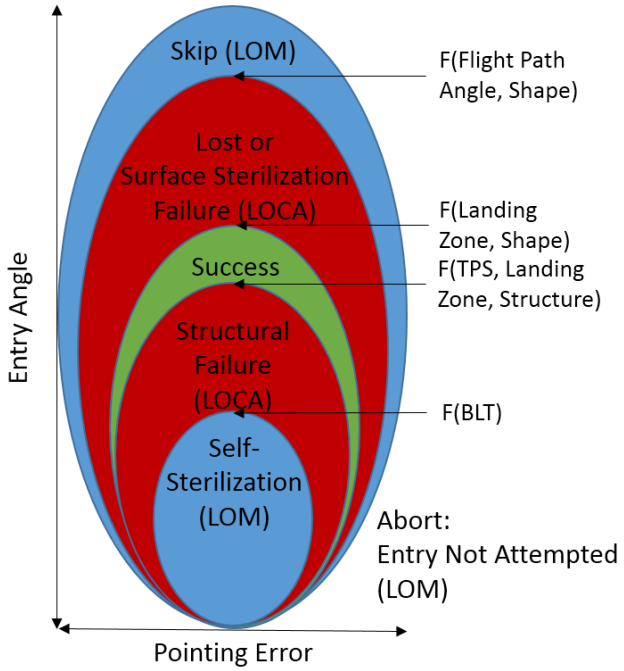

Fig. 8. Conceptual diagram of the interplay between design parameters, failure thresholds, and the risks of both LOCA and LOM.

IV. RESULTS

The model was used to produce results based upon nominal ETM conditions, which were calculated such that ballistic propagation from ETM leads to the EI conditions in Table II, including dispersions. The baseline dispersions used for each parameter at the ETM and during EDL are based upon data from previous missions and analyses[4,7,20] and are shown in Table III.

TABLE III. Baseline parameter dispersions.

Parameter	**Range**
Radial Velocity [e_r]	±0.1%
Theta Velocity [e_θ]	±0.1%
Phi Velocity [e_φ]	±0.1%
Radial Distance [r]	±0.1%
Theta [θ]	±0.075 deg
Phi [φ]	±0.075 deg
Mass	±0.75 kg
Drag Uncertainty	±10%
Convective Heating	100% – 170%
Radiative Heating	100% – 250%
TPS Density	±4%
TPS Heating Coefficient	±5%
TPS Conductivity	±5%

Nominal mission results are produced and examined to establish the connection between mission success and meeting the planetary protection reliability goal. Sensitivities to dispersion parameters are studied to provide insight into what drives the risk of each failure threshold. The sensitivity of the failure probability estimates to the risk-driving thresholds is then investigated. These sensitivity results are then used to examine whether a given architecture could feasibly meet the key design and performance parameters needed to achieve the reliability goal using existing technologies.

IV.A. Nominal Results for LOM and LOCA

Nominal results (i.e., results for a nominal mission without parameters dispersions) indicate that a successful sample return is likely, given a fully functional bus and undamaged EEV at ETM. A nominal mission will incur only LOCA risk from the SRF. Figure 9 shows the nominal results. These results only include risk of LOM stemming from hardware unreliability and MMOD and LOCA risk from the SRF, which meets the planetary protection reliability goal. These estimates have been produced by only considering key components identified in previous studies[5] and assuming minimal redundancy. These components are exposed to dormant failure rates[21] for the entire 13.5-year mission duration.

Results that include baseline parameter dispersions were produced by assuming a uniform distribution for all parameters. Figure 10 shows the total LOM risk including the LOCA risk for the nominal mission with dispersions. These results indicate a very large number of failures due to the EEV entering Earth's atmosphere at an excessively shallow entry angle and skipping back out into heliocentric orbit. While not a contributor to LOCA, this failure mode is a significant contributor to LOM.

Figure 11 shows the risk results for LOCA with dispersions included. As the bounds and distribution of these dispersions are conservative and do not do reflect an actual design, the corresponding probabilistic estimates are also conservative. However, these results do indicate how the baseline parameters should be enhanced to achieve the planetary protection reliability goal. The indicated enhancements are to increase TPS thickness to reduce the BLT at landing, or to refine the criteria for structural failure on landing, based on the qualities of the landing point and the strengths of the structure at the maximum BLT at landing.

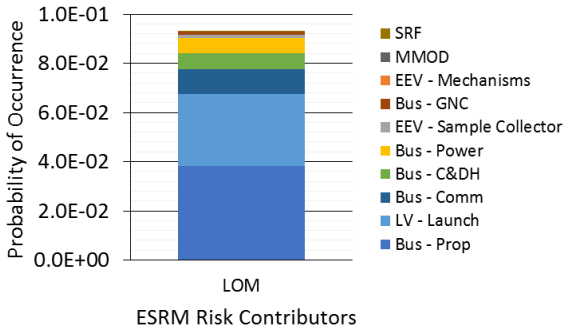

Fig. 9. Risk of LOM for nominal mission without dispersions.

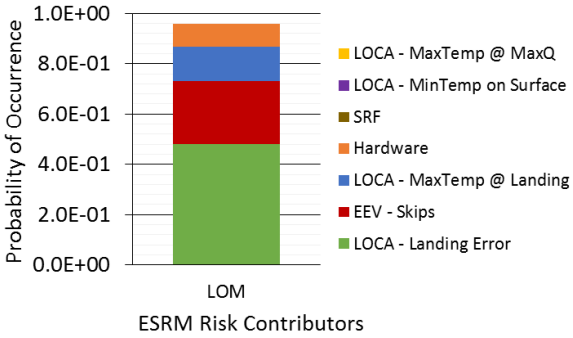

Fig. 10. Risk of LOM with dispersions and baseline failure thresholds.

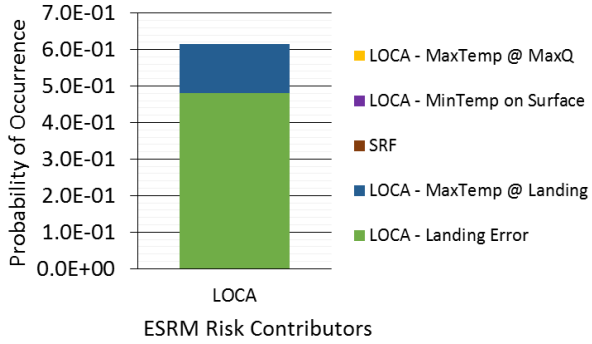

Fig. 11. Risk of LOCA with dispersions and baseline failure thresholds.

The nominal results with the initial assumptions do not meet the planetary protection reliability goal. Thus, additional model refinement is required to further investigate the risk-driving sources of design and performance uncertainty included in the model. Better understanding of this uncertainty will aid in determining whether the model is overly conservative or the planetary protection goal itself is not achievable with current technology.

IV.B. Sensitivity at Earth Target Maneuver

Sensitivity sweeps beyond the baseline dispersion limits, centered about the nominal values, were modeled by varying a single parameter at a time. This aids in understanding which dispersion parameters drive the LOCA risk and require enhancement to meet the planetary protection reliability goal, and which parameters can be left as conservative placeholders without impacting the results. Results are displayed relative to the baseline threshold value for each failure parameter. Parameters below 100% indicate a successful outcome, except for Minimum Surface temperature, which must be above 100% for a successful outcome to occur. This demonstrates the impact each dispersion parameter has on the available threshold margin. Sensitivities of the failure parameters to radial velocity and theta velocity at ETM are presented here. All other dispersion parameters in Table III were also investigated. Aside from Phi Velocity, which produced similar results to those presented, the dispersion parameters not discussed here did not affect failure probability.

Figure 12 shows the sensitivity of the four LOCA failure parameters to the radial velocity after the ETM. If the radial velocity falls below -11.92 km/s, the EEV will skip out of the Earth's atmosphere and enter heliocentric orbit instead of returning to Earth, which is assumed not to cause LOCA but does cause a LOM. These results indicate that the final landing point and the maximum BLT at landing are sensitive to the radial velocity. Thus, the performance of the GNC equipment and the EEV separation system mechanism will be vital to the success of the mission.

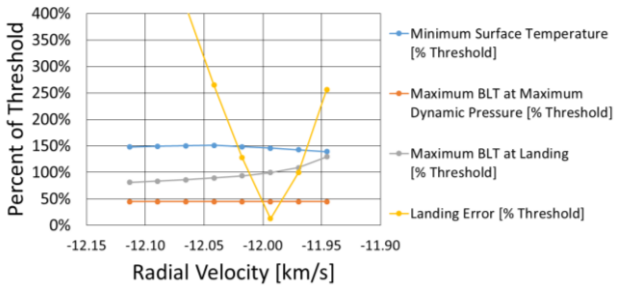

Fig. 12. Sensitivity of LOCA failure criterion parameters to radial velocity at ETM.

Figure 13 shows the sensitivity of the four LOCA failure parameters to theta velocity at the ETM, representing a pointing error after EEV separation. Again, landing error is extremely sensitive to this value, as is the maximum BLT at landing. This sensitivity demonstrates the importance of a properly aligned velocity vector upon EEV release. This further indicates the importance of a precise GNC sensing system, and that the EEV release mechanism must have very narrow dispersion about the imparted energy.

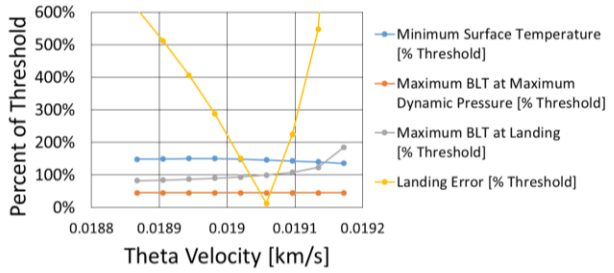

Fig. 13. Sensitivity of LOCA failure criterion parameters to theta velocity at ETM.

Overall, the results indicate that these dispersions at ETM drive the LOCA risk of landing error with some impact on the BLT at landing. The other thresholds are relatively insensitive to these dispersions.

IV.D. Sensitivity During Entry, Descent, and Landing

Figure 14 shows the sensitivity of the four LOCA failure parameters to uncertainty in the drag predictions used for the analysis, as a function of percentage of the nominal drag value. The results indicate that landing error is somewhat sensitive and drag error could impact results, depending on the specific state of the vehicle in a particular realization, but drag error alone is not enough to trigger a failure. In addition, the minimum surface temperature is slightly sensitive and the margin above the necessary sterilization temperature is reduced with increased drag error, but again, drag error alone is not enough to trigger a failure.

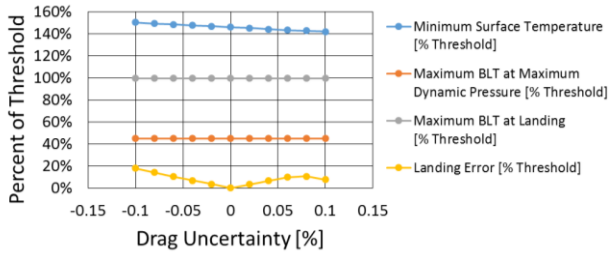

Fig. 14. Sensitivity of LOCA failure criterion parameters to EDL drag predictions.

Figure 15 shows the sensitivity of the four LOCA failure parameters to the convective heating uncertainty in FIAT, which represents an experimentally derived factor applied to the analytic prediction of convective heating. The parameter effectively amplifies the heat transfer from the environment to the surface. With an error factor of unity, the maximum BLT at landing threshold is just under 100%, leaving very little margin for increases in convective heating.

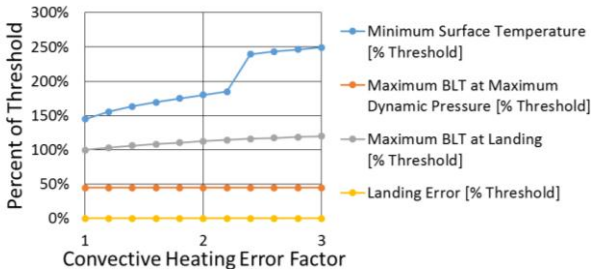

Fig. 15. Sensitivity of LOCA failure criterion parameters to convective heating uncertainty.

The results show that both the landing error and maximum BLT at MaxQ are insensitive to this parameter. The minimum surface temperature is highly sensitive, but the predicted value increases with greater uncertainty in the heating estimate, further assuring that the surface will be sterilized. The maximum BLT at landing is also sensitive to this parameter and could increase the likelihood of failure without other parameter variations. These results indicate that reducing the uncertainty of the convective heating of the TPS would increase the estimated likelihood of mission success.

Generally, the results indicate that minimum surface temperature and maximum BLT at landing are sensitive to the uncertainties during EDL, including the performance of the TPS. The maximum BLT at MaxQ and landing error are not sensitive to these parameters.

IV.B. Sensitivity of LOCA Risk Driver Results

The probabilities of LOM and LOCA are both heavily influenced by the assumed threshold values selected for each failure criterion parameter. While using failure threshold parameters is a valid approach to bound system risks, it effectively obfuscates the actual capability of the system to perform successfully. The threshold values are generally quite conservative because the analyses that produce them often stack worst-case assumptions on top of worst-case assumptions. A sensitivity study is performed to determine the degree to which each failure threshold must be relaxed to yield a LOCA probability of less than 1 in 1,000,000.

Figure 16 shows the sensitivity of the LOCA probability results to the temperature threshold for structural failure at landing. This risk estimate benefits from the internal self-sterilization threshold BLT, which prevents LOCA if exceeded prior to landing. With increased BLT at landing, the likelihood of structural failure on impact increases due to the weakened state of the EEV. The processes by which the structure would fail are dependent upon the characteristics of the landing location and the state of the structure protecting the sample.

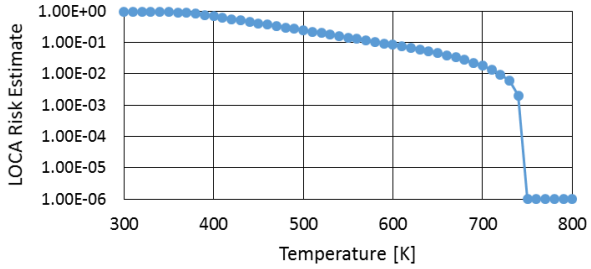

Fig. 16. Sensitivity of LOCA risk estimates to the temperature threshold for structural failure at landing.

To reduce the risk contribution of this threshold, the modeling assumptions that impact the BLT could be refined. However, since it is unlikely that the structure would be able to withstand temperatures up to 800 K, an increase in model fidelity is required to more precisely capture the physical interaction of the system structure with the physical properties of the specific landing site in each realization. By physically modelling the interaction of the system with the precise landing site, the failure threshold parameter can be removed, allowing the risk model to capture the inherent robustness of the design.

Figure 17 shows the sensitivity of the LOCA probability to the landing error threshold. These results indicate that the baseline ETM dispersions are unacceptable and must be enhanced, given the extreme range of the landing errors (up to 450 km) that would have to be accommodated to effectively reduce this risk contribution.

Figure 18 shows the sensitivity of LOCA probability to the minimum surface sterilization temperature threshold. The baseline peak value required to sterilize the vehicle is nominally set at 398 K, leading to zero probability of not successfully sterilizing the surface during the Monte Carlo simulation. Applying a pessimistic bound of 773 K, however, leads to a failure every time. This extreme sensitivity indicates the importance of understanding the EEV surface sterilization requirements. Moreover, the simple failure threshold criteria may prove to be too conservative and require a time-history of the physical process to determine whether a sterilization failure would occur.

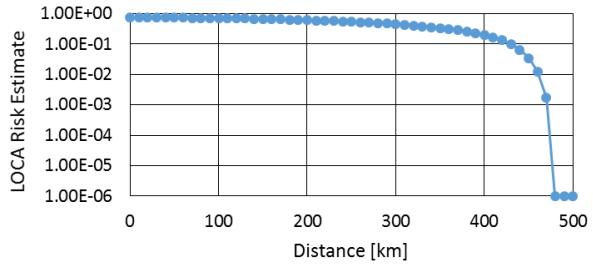

Fig. 17. Sensitivity of LOCA risk estimates to structural failure at landing due to landing error threshold.

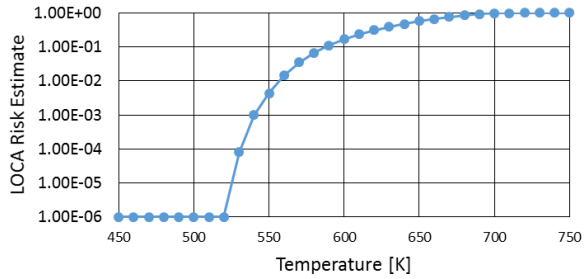

Fig. 18. Sensitivity of LOCA risk estimates to minimum surface temperature threshold for sterilization failure.

Overall, these sensitivity results indicate that an extreme amount of relaxation of the constraints would be necessary to achieve the planetary protection reliability goal. Thus, exploring other avenues of risk reduction, such as reducing dispersions or increasing capabilities, is likely to be more successful.

IV.E. Design and Performance Parameters Required to Achieve Planetary Protection Reliability Goal

The sensitivity study results were used to create an enhanced, more representative set of performance parameter dispersions and an increased TPS thickness that together would meet the planetary protection reliability goal. The TPS thickness was increased by 34% from 3.05 cm to 4.08 cm to address excessive BLT, due to uncertainties in TPS performance, causing structural failures at landing. This increased TPS thickness and enhanced set of model dispersions yielded zero failures in 1.2 million Monte Carlo realizations using the baseline failure thresholds. Table IV gives the enhanced dispersions and the percentage by which they were modified relative to the baseline values. All other parameters were left at the baseline values. A normal distribution, with the parameter range as the three-sigma value, is used for all parameters at the ETM and log-normal distributions are used for the EDL parameters.

The enhanced parameter dispersions indicate that an order of magnitude improvement over the current state-of-the-art would be necessary to meet the reliability goal, given the nominal failure threshold values. Such an improvement in the error in EEV state at ETM could prove to be extremely challenging, but could reasonably be considered possible with current technology.

TABLE IV. Enhanced Parameter Dispersions.

Parameter	**Range**	**Relative**
Radial Velocity [e_r]	±0.01%	10%
Theta Velocity [e_θ]	±0.01%	10%
Phi Velocity [e_φ]	±0.01%	10%
Radial Distance [r]	±0.01%	10%

The required increase in TPS thickness necessary to meet the reliability goal with the nominal failure threshold values represents a potentially dramatic increase in EEV mass. Such a design enhancement would be extremely challenging, as the total TPS mass could grow to as high as 36.2 kg or 91% of the EEV mass. This would leave almost no mass available for mechanisms, structure, or payload. Moreover, such a thick carbon-phenolic TPS has never been flown by NASA and may introduce additional, unknown failure modes that are not currently included in this risk model. This indicates that, given the current modeling assumptions, the planetary protection reliability goal would be a challenge to achieve with current technology and could benefit from future TPS technology development.

V. CONCLUSIONS

The results presented are driven in large part by the baseline dispersions of the parameters used by previous missions and the use of binary failure thresholds. The failure thresholds do not capture the full robustness of the design and do not lead to a reliability estimate that meets the planetary protection reliability goal with the baseline design and performance parameters. Reducing the parameter dispersions and increasing the robustness of the TPS design does lead to a system that meets the planetary protection reliability goal and shows that such a mission could be feasible. However, these design enhancements may not be achievable with current technology.

Thus, the complexity of the model must be increased to more precisely determine the degree to which current performance and design expectations must be enhanced to meet the planetary protection reliability goal. This can be achieved by further coupling the existing simulations to include a physics-based model of structural response during landing. Including additional fidelity in the model's dynamic framework will refine the conservative assumptions, produce a more accurate risk assessment, and better capture the inherent robustness of the design.

Such a model could explore alternate concepts and assess their potential to meet the planetary protection reliability goal by giving the design team the ability to

trade reductions in LOCA for increases in LOM using the available design and performance parameters—e.g., flight path angle, EEV shape, TPS stack-up, abort criterion, and self-sterilization BLT. For example, by tuning the nominal return trajectory and the response of the vehicle to increases in BLT, a less robust TPS design could be implemented with very narrow margins for a successful outcome. This narrow window of success would correspondingly shrink the very undesirable outcome of LOCA and would lead to a great many more missions that would end with internal self-sterilization or with the EEV skipping off of Earth's atmosphere into heliocentric space.

Ultimately, due to the extreme constraints placed upon the system to protect the Earth's biosphere from sample release, risk-informed design should be implemented in an ESRM project as early as initial conception. Due to the highly time- and state-dependent interactions between the EEV and the environment, a dynamic, physics-based PRA should be employed in order to most accurately capture the key risk factors and produce results to guide and optimize the design.

REFERENCES

1. J. H. WAITE, "Liquid water on Enceladus from observations of ammonia and 40Ar in the plume," *Nature*, **460**:487–490 (2009).
2. P. TSOU, et al "LIFE - LIFE: Life Investigation for Enceladus, A Sample Return Mission Concept in Search for Evidence of Life," *Astrobiology*, **12**, 8 (2012).
3. Mars Sample Return Issues and Recommendations, Space Studies Board, National Research Council, National Academy of Sciences (2097).
4. J. R. FRAGOLA, B. P. PUTNEY, J. W. MINARICK, III "Mars Sample Return Probabilistic Risk Assessment Final Report," SAIC, Rockville Centre, NY (2002).
5. C. N. NIEBUR, et al "Planetary Science Decadal Survey, JPL Rapid Mission, Enceladus Study Final Report," Jet Propulsion Laboratory, California Institute of Technology (2010).
6. R. BRAUN, et al, "Mars Sample Return Earth Entry Vehicle, Conceptual Design Assessment," NASA Langley Research Center, Hampton, VA (1999).
7. P. N. DESAI and G. D. QUALLS, "Stardust Entry Reconstruction," *Journal of Spacecraft and Rockets*, **47**, 5 (2010).
8. J. Y. RICHMOND and R. W. MCKINNEY (editors), "*Biosafety in Microbiological and Biomedical Laboratories*," Centers for Disease Control and Prevention, Atlanta, Georgia (1999).
9. S. GO, D. L. MATHIAS, C. J. MATTENBERGER, S. LAWRENCE, K. GEE, "An Integrated Reliability and Physics-based Risk Modeling Approach for Assessing Human Spaceflight Systems," *Probabilistic Safety Assessment and Management conference*, Honolulu, HI (2014).
10. S. A. MOTIWALA, D. L. MATHIAS, C. J. MATTENBERGER, "Conceptual Launch Vehicle and Spacecraft Design for Risk Assessment", NASA/TM-2014-218366, (2014).
11. C. R. HARGRAVES and S. W. PARIS, "Direct Trajectory Optimization Using Nonlinear Programming and Collocation," *AIAA Journal of Guidance, Control, and Dynamics*, **10**, 4 (1987).
12. "U.S. Standard Atmosphere, 1967," NASA-TM-X-74335, Washington, D.C. (1976).
13. "Cart3D: Software and User Manual for Cart3D," http://people.nas.nasa.gov/~aftosmis/cart3d/, NASA.
14. D. J. KINNEY, "Aero-Thermodynamics for Conceptual Design", AIAA Paper 13382 (2004).
15. Y. -K. CHEN and F. S. MILOS, "Ablation and Thermal Response Program for Spacecraft Heatshield Analysis," *Journal of Spacecraft and Rockets*, **36**, 3 (1999).
16. E. VENKATAPATHY et al, "Selection and Certification of TPS: Constraints and Considerations for Venus Missions", *6th International Planetary Probe Workshop*, Atlanta, GA, Georgia Institute of Technology (2008).
17. D. L. PETERSON and W. E. NICOLET, "Heat Shielding for Venus Entry Probes," *Journal of Spacecraft and Rockets*, **11**, 6 (1974).
18. E. J. WEILER, "Planetary Protection Provisions for Robotic Extraterrestrial Mission," NPR 8020.12D, Science and Mission Directorate (2005).
19. M. LO et al, "Genesis Mission Design," AIAA 98-4468, *AIAA/AAS Astrodynamics Specialist Conference*, Boston, MA, August (1998).
20. A. M. CASSELL et al, "Hayabusa Re-entry: Trajectory Analysis and Observation Mission Design", AIAA 2011-3330, *42nd AIAA Thermophysics Conference*, Honolulu, HI (2011).
21. B. C. REISTLE, "Generic Risk Analysis Data Set," NASA Johnson Space Center Safety & Mission Assurance, contact: bruce.c.reistle@nasa.gov (2014).