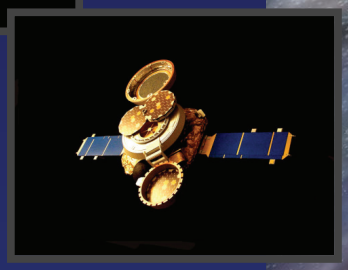
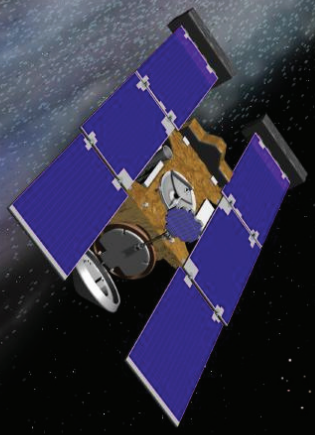
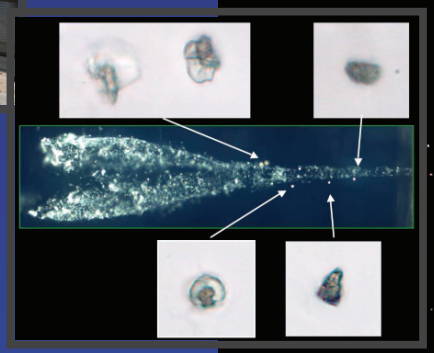



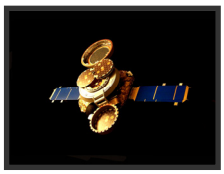


# Sample Return Primer & Handbook

January 2007
JPL D-37294




Columbia Accident Investigation Board logo

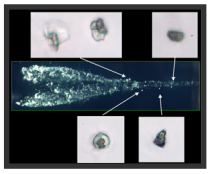


Genesis spacecraft in solar wind collection configuration

Stardust sample return capsule as captured by NASA's DC-8 Airborne Observatory

Stardust sample return capsule on the desert floor of the Utah Test and Training Range

Donald Brownlee, principal investigator with the University of Washington, and Friedrich Horz, Johnson Space Center, get a close look at the Stardust sample collection grid



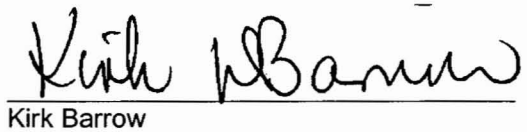
Cross-section of a Comet Wild 2 particle track in aerogel

# Sample Return Primer and Handbook

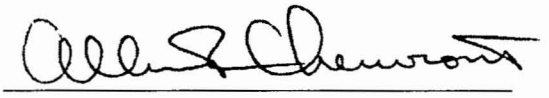
## Table of Contents

# Sample Return Primer and Handbook

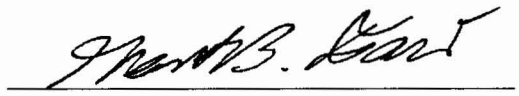
**Prepared By**



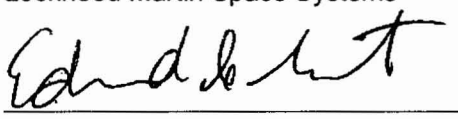
Kirk Barrow
System Safety
Jet Propulsion Laboratory



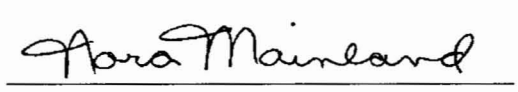
Allan Cheuvront
Spacecraft Systems
Lockheed Martin Space Systems



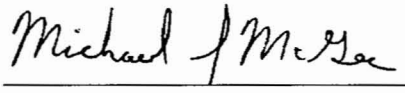
Grant Faris
Mission Assurance
Jet Propulsion Laboratory



Edward Hirst
Mission Systems
Jet Propulsion Laboratory

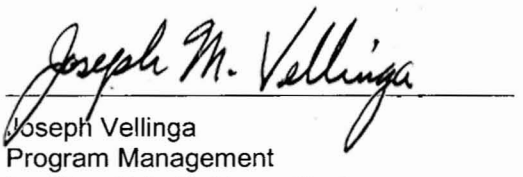


Nora Mainland
Mission Operations
Jet Propulsion Laboratory

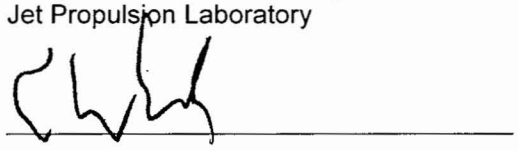


Michael McGee
Recovery Operations
Lockheed Martin Space Systems

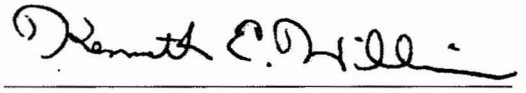
Christine Szalai
Entry, Descent, and Landing
Jet Propulsion Laboratory



Joseph Vellinga
Program Management
Lockheed Martin Space Systems

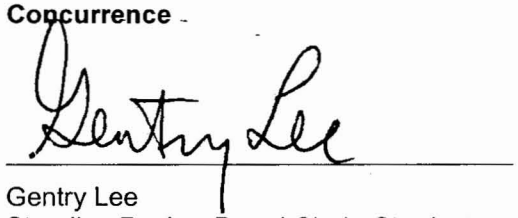


Thomas Wahl
Project Systems Engineering
Jet Propulsion Laboratory

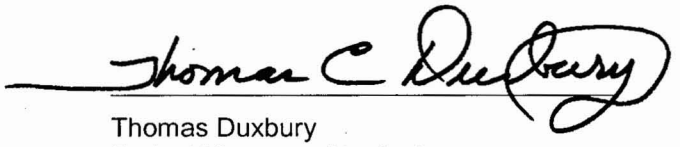


Kenneth Williams
Navigation
Jet Propulsion Laboratory

**Concurrence**



Gentry Lee
Standing Review Board Chair, Stardust
Jet Propulsion Laboratory



Thomas Duxbury
Project Manager, Stardust
Jet Propulsion Laboratory

# Acknowledgements

The Sample Return Primer and Handbook (SRPH) authors would like to acknowledge the support of a number of groups and individuals who made possible the creation of this document and/or contributed to its successful completion.

Michael Ryschkewitsch, Chairman of the Genesis Mishap Investigation Board, co-chair of the Stardust Risk Review, and participant in several other Stardust reviews – A debt of gratitude is owed for his strong advocacy and support for the development of this document. His efforts are responsible for obtaining the funding that made possible this undertaking.

Gentry Lee, Review Board Chair for both the Genesis and Stardust risk assessment and readiness review processes – His broad, in-depth, experienced, and visionary guidance was invaluable during the architecting and refinement of many of the processes, plans and procedures captured within these pages.

The SRPH sponsors – Andrew Dantzler, former Director, Planetary Science Division, Science Mission Directorate; Douglas McCuistion, Director, Mars Exploration Program, Planetary Science Division, Science Mission Directorate; Garry Lyles, Director, Constellation Systems, Exploration Systems Mission Directorate – for providing the actual funding to support this task.

The SRPH contributors and reviewers - William Blume, Dennis Byrnes, Al Cangahuala, Dennon Clardy, Prasun Desai, Dwight Eckert, Larry Ellis, Abigail Ettinger, Merrilee Fellows, Sandy Fruend, Michael Galuska, Kevin Gilliland, Ken Gowey, Janis Graham, Terry Himes, Dale Howell, Mark Ivanov, David Jefferson, John Klein, Wayne Lee, Lisa Ling, George Lewis, Karen Liao, Charles Love, Ben Lucas, Steven McClard, Gavin Mendeck, Frank Mortelliti, Brian Muirhead, Mary Beth Murrill, Jim Neuman, Marilyn Newhouse, Priscilla Parrish, David Perkins, Chuck Pfaeffle, Ahmed Salama, Adrian Segura, Kuei Shen, Pete Spidaliere, Don Sweetnam, Jeff Tooley, Bill Willcockson – for contributing to the accuracy and completeness of the contents herein.

The Stardust and Genesis Project independent reviewers, who are too many to list, but whose unwavering attention to detail from lengthy review to lengthy review provided a much needed sounding board and kept plans and efforts on the true and proper path.

And last but not least, the Stardust and Genesis Jet Propulsion Laboratory and Lockheed Martin Space Systems flight and recovery teams; and all organizations that supported the risk and readiness processes, and actual flight and recovery operations –

Aerospace Corporation
Ames Research Center, Space Technology
Dugway Proving Grounds
Hill Air Force Base
Johnson Space Center, Astromaterials Research and Exploration Science
Johnson Space Center, Flight Design and Dynamics
Langley Research Center, Space Systems
Pioneer Aerospace
South Coast Helicopters, Inc.
United States Strategic Command
Utah Test and Training Range
Vertigo, Inc.

- their commitment to excellence is captured in these pages for the use of future generations of scientists and engineers.

# Executive Summary

In early January 2005, the Stardust Project was a year past its encounter with the comet Wild 2 and its successful capture of particles from the comet. The project was also a year away from the return of those sample particles to the salty deserts of the Utah Test and Training Range. Stardust had spent the bulk of its mission in quiescent cruise and then had executed its comet encounter without much fanfare, its close flyby of Wild 2 having been overshadowed by the arrival and landing of the first Mars Exploration Rover at the Red planet. The Stardust Earth return and sample recovery road map laid out six years earlier had not anticipated that significant attention would be focused on its return and recovery activities and that approved plans would come under new scrutiny from an altered perspective. However, in the years since Stardust had been launched, there had been a significant change in the management culture throughout the National Aeronautics and Space Administration (NASA), including the Jet Propulsion Laboratory (JPL). Because of the Columbia shuttle accident and, especially, the Genesis landing mishap as it returned with its solar wind sample, Stardust received much more management and external engineering attention than had originally been expected. So in early 2005, Stardust was required to construct, and then follow, a careful, thorough risk management process that identified and communicated all significant risks and safety measures associated with its return and recovery.

The Stardust Project was the fourth mission selected by NASA's Discovery program. The mission's primary objective was the collection and return to Earth of particle samples from the comet Wild 2, with secondary objectives that included the collection and return of samples from the interstellar dust stream. The core mission team was comprised of the Principal Investigator located at the University of Washington, JPL providing project management, systems engineering and mission operations, including mission design, navigation and mission operations assurance, and Lockheed Martin Space Systems (LMSS) providing the flight system, spacecraft operations, and recovery operations. Several support organizations were essential during return operations, including the Department of Defense's Utah Test and Training Range (UTTR), Dugway Proving Grounds, and United States Strategic Command, and the Johnson Space Center's Astromaterials Research and Exploration Science Division.

The Stardust mission was launched in February 1999. An Earth gravity assist flyby in January 2001 set up the encounter with comet Wild 2 in January 2004. Interstellar dust collection occurred during selective periods of cruise when the spacecraft velocity was aligned with the interstellar dust stream. After a total flight of 7 years and 4.6 billion kilometers (2.9 billion miles), Stardust returned to Earth on January 15, 2006, and successfully delivered the sample return capsule to within 10 kilometers (6.2 miles) of the intended landing target. Ground operations to recover the capsule and transfer all flight hardware, samples included, to the curatorial facilities at Johnson Space Center were executed without incident. Initial examination of the perfectly preserved sample tray revealed a bounty of dust samples, both comet and interstellar in origin, for the considerable benefit of the global science community.

While Stardust was on its way to Wild 2, the Columbia Accident Investigation Board (CAIB) issued a report that engendered a cultural change within the NASA community with respect to the processes by which both engineering and programmatic risks are identified, assessed, mitigated, and, equally importantly, communicated with all levels of management. In addition, the many similarities between the Stardust and Genesis projects created a direct need for Stardust to respond to recommendations provided by the still in process Genesis mishap investigation. Specifically, since the design of the Genesis sample return capsule was derived from the earlier design of the Stardust return capsule, and since Genesis had also returned to UTTR (although Genesis launched AFTER Stardust, its Earth return preceded the Stardust return), there was a requirement that the Stardust Earth return and recovery plan address the preliminary findings of the Genesis Mishap Investigation Board (MIB).

Responding to both the CAIB report and the as yet unfinished findings of the MIB, JPL and the Stardust Project management team developed and implemented a comprehensive task plan for the Earth return and recovery phases of the Stardust mission. The fundamental framework of the plan was a series of independent risk reviews that started with an examination of the details of the Stardust spacecraft at the component level (including plans, requirements, and test results), and proceeded through subsystem risk reviews conducted by peers to system level risk and readiness reviews. The project's plan, however, was far more than a carefully considered series of reviews. The implemented plan infused into the project a veritable paradigm shift in the way that risks were considered. The completion of this plan allowed the project to properly communicate Earth return and recovery residual risks to upper management and to achieve the required state of readiness in hardware, software, and personnel to conduct robust sample return and recovery operations.

Immediately after the successful return and recovery of the Stardust sample capsule, a wave of support began to build for documenting the final year of activity on the Stardust Project. There was a widespread desire to capture, in effect, the entire Earth return and recovery process - what was done, why it was done, and whether it worked – and by so doing provide a primer for planning and implementing the return and recovery phases of future sample return missions. With the strong support of key, high-level, members of the Stardust Standing Review Board, including the chairman of the Genesis MIB, funding was obtained for this Sample Return Primer and Handbook from three different elements of the NASA family: the Discovery Program Office and the Mars Exploration Program of the Planetary Science Division, Science Mission Directorate, and Constellation Systems in the Exploration Systems Mission Directorate.

This three-part Sample Return Primer and Handbook provides a road map for conducting the terminal phase of a sample return mission. The main chapters describe element-by-element analyses and trade studies, as well as required operations plans, procedures, contingencies, interfaces, and corresponding documentation. Based on the experiences of the lead Stardust engineers, the topics include systems engineering (in particular range safety compliance), mission design and navigation, spacecraft hardware and entry, descent, and landing certification, flight and recovery operations, mission assurance and system safety, test and training, and the very important interactions with external support organizations (non-NASA tracking assets, landing site support, and science curation).

Many challenges were faced during the implementation of the new Stardust plan for preparation for the Earth return and recovery. All of the challenges, and action to respond to them, were weighed from the point of view of risk. Some of the major challenges addressed by the Stardust team during the implementation of the plan are presented below:

- Insufficient prior interaction between the navigation team and the attitude control team in the specification of maneuver error modeling led to the need for an error model re-certification effort. This effort was aided by the return of development phase engineers familiar with the pre-launch requirements verification and validation work.

- Avoidance of the entry trajectory's orbital plane intersection with population centers, in terms of the progression of the instantaneous impact point, eased compliance with Earth return range safety requirements (risk to population and property) and enabled the use of easily defensible spacecraft reliability arguments. However, break-up and burn-up analysis tools for small vehicles lack a comfortable set of real-world data to provide proper verification and validation. Sensitivity analyses were conducted to characterize the risks of the analysis being incorrect.

- A rigorous and thorough test and training program to validate the operational plans was invaluable for this multi-faceted, complex system. As a result of the testing, for example, fundamental errors and omissions were discovered in the entry decision criteria architecture and then corrected before the actual entry decision was made.

- Understanding of spacecraft capabilities that exceeded the design requirements was essential to achieve an understanding of risk and allow proper risk balance. However, operational use of capabilities beyond requirements required certification. In order to designate the entire UTTR as available for landing the sample return capsule, the tolerable entry flight path angle error was doubled through a rigorous re-certification effort.

- Validation and verification test efforts were most valuable when they re-created the flight-like environment. Risk assessment tests to certify that the Stardust deceleration switches would operate correctly led to out-of-specification results until test setups were used that properly simulated the expected vibrations of the entry, descent, and landing.

- External agencies benefited from early and regular interaction during the planning and preparation process. Stardust was only one part of their very busy and full operational portfolio. It was challenging to get the full attention of the required organizations during the test and training process, and the project was not always successful.

- The human participation in recovery operations required particular attention to ensure that human safety was the number one priority. All credible contingency scenarios were identified, documented, and rehearsed. Extensive interaction with independent, institutional and agency safety representatives was progressively added to project plans, including in-the-field observation during test and training.

This primer, Chapters 2 through 11, describes the risk assessments, analyses, and reviews performed in the final year before Stardust's return, which were necessitated by a revised set of Earth entry and risk communication requirements. With this foreknowledge, future sample return missions should be able to address how to more efficiently achieve requirements compliance and mission robustness. For example, much of the required work would benefit from expertise that is readily available during pre-launch development and implementation phases. Then, the pre-return phase might only resurrect that work and focus on what has been learned about the flight system during the mission.

In addition to the early primer chapters, which are designed to be generic and as applicable as possible to a wide class of sample return missions, this primer also contains complementary appendices designed to capture a more specific Stardust set of lessons learned. It is hoped that these observations will also be useful for future sample return efforts. Finally, an accompanying compact disc provides a copy of the Stardust Project Library, thereby permitting the interested reader to have access to all of the documentation and independent review material relevant to the final year of the Stardust mission. It was from this raw material, and the reflections of the key participants in this historic space endeavor, that this primer was derived.

May the future of sample return benefit from the knowledge captured within these pages.

# Chapter 1: Overview

The Stardust mission was the fourth selected in the National Aeronautics and Space Administration's (NASA) Discovery Program, which provides a competitive avenue for scientists to partner with NASA and industry in the pursuit of low-cost, highly focused planetary science investigations. Selected in late 1995, the Stardust spacecraft and mission implementation was performed as a joint venture between NASA, the University of Washington (the Principal Investigator's home institution), the Jet Propulsion Laboratory (JPL), and Lockheed Martin Space Systems (LMSS).

The primary science goal of the mission was to collect particles from a pristine comet. 81P/Wild 2 was selected as the target because its orbit had only recently been altered by a close flyby with Jupiter (1974) from one with perihelion at Jupiter solar distance where it had been preserved in its primordial state to one with aphelion at Jupiter distance where it could be reached with available space technology. Secondary and tertiary science objectives included in-situ science during the comet flyby (images, dust mass spectrometry, and dust flux quantization) and capture of interstellar dust during cruise.

Stardust's flight mission, illustrated in Figure 1-1, began with launch from Cape Canaveral Air Force Station, Florida on a trajectory that took it three times around the Sun before returning to Earth on January 15, 2006. It took the spacecraft five years, two and a fifth orbits around the Sun, inclusive of an Earth gravity assist and three deep space maneuvers, to arrive at the time and place of its encounter with Wild 2 on January 2, 2004. En route to the comet, Stardust set a record for operating the farthest from the Sun for a solar powered vehicle, flew past a remote asteroid to practice its comet flyby, and captured interstellar dust during periods of the orbit where relative velocities were favorable.

The Stardust spacecraft, illustrated in Figure 1-2, was designed to operate its full instrument suite during the comet encounter, and operate on minimal power at maximum solar range. Spacecraft components were either block or string redundant, with the exception of the rechargeable spacecraft battery, mechanisms (solar array and sample return capsule (SRC) retention and release, collector deployment) and science instrumentation.

Stardust's cosmic treasure was returned to Earth in a SRC, also illustrated in Figure 1-2. The comet and interstellar dust particles were captured in a grid of innovative material called aerogel. Aerogel is a silicon-based solid with a porous, sponge-like structure in which 99.8 percent of the volume is empty space. One thousand times less dense than glass, having established a record for the lightest known material, it was ideally suited for slowing down and capturing intact comet and interstellar dust particles, which were traveling at a speed of 6.1 (13,600) and >10 kilometers per second (22,400 miles per hour), respectively.

## Earth Return

The Stardust Earth return phase spanned a period just under two weeks in duration. Return activities began with the execution of a trajectory correction maneuver (TCM) ten days before entry, and ended, for the ground teams, with delivery of the SRC to the curatorial facility at Johnson Space Center (JSC). For the flight team, the return phase concluded with placing the spacecraft bus in a safe state and on a long term decommissioning trajectory.

Figure 1-3 shows an overview of the flight mission timeline. This plan was geared toward ensuring proper targeting and delivery of the SRC to the selected landing location while complying with NASA and Utah Test and Training Range (UTTR) range safety requirements and balancing the risk associated with unplanned, untoward events (for example, entry into safe mode at an inopportune moment). For Stardust, safe mode entries were particularly egregious due

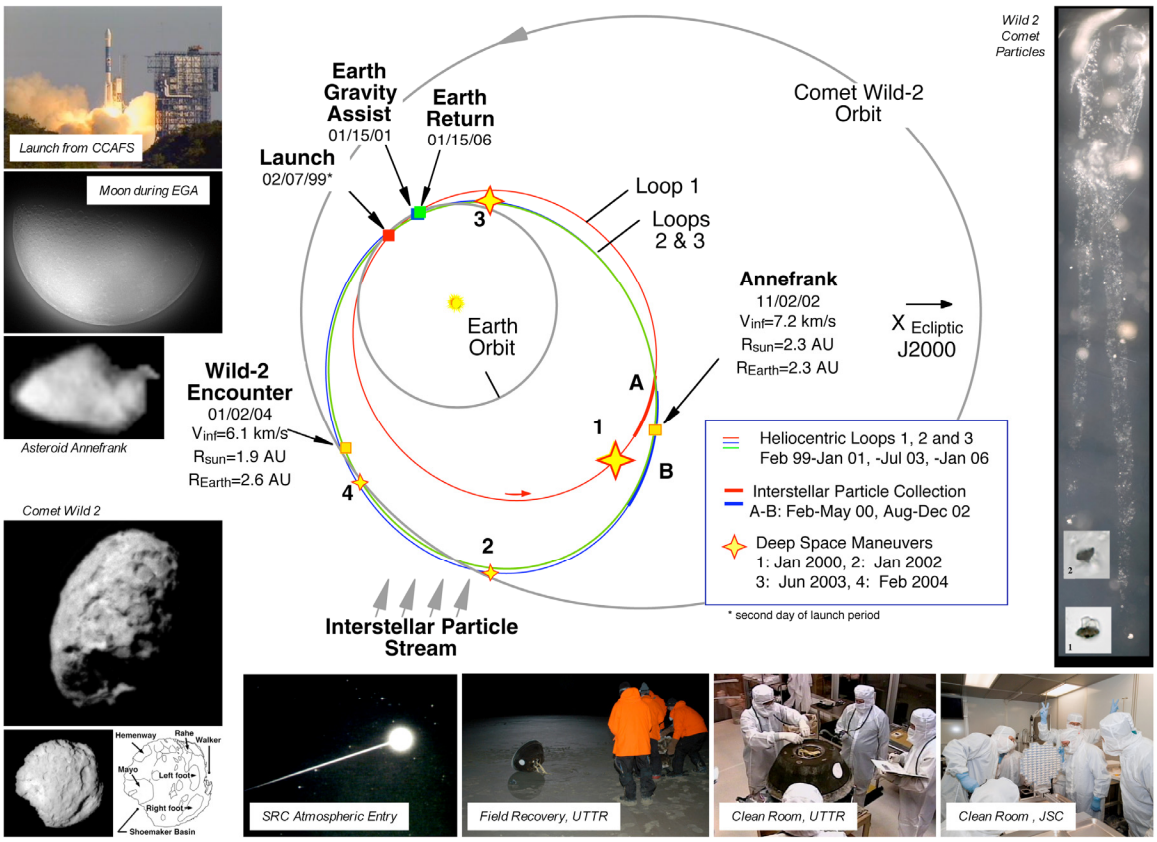



**Figure 1-1. Stardust Flight Mission**

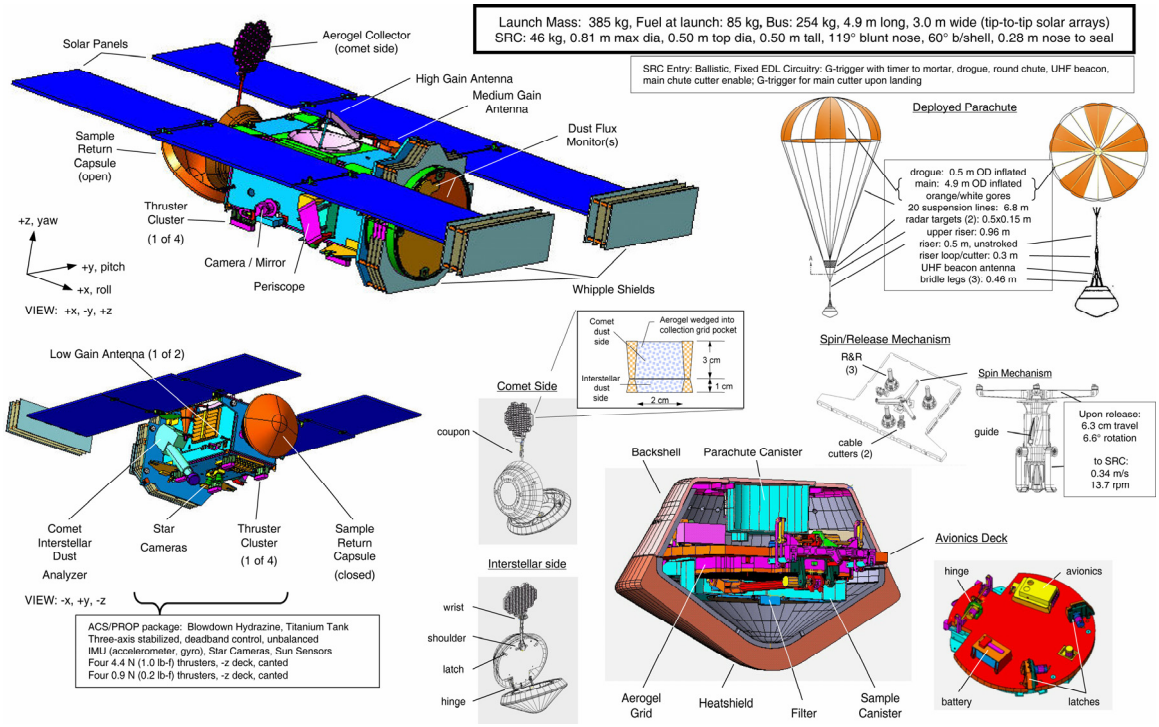



**Figure 1-2. Stardust Flight System**

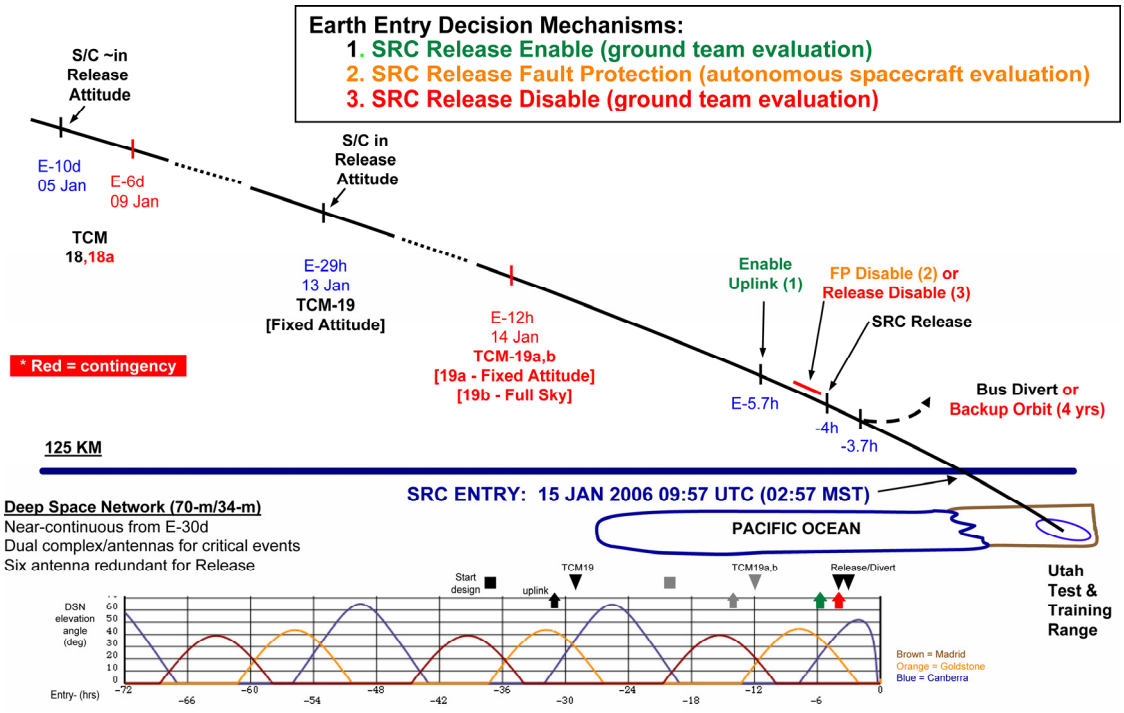
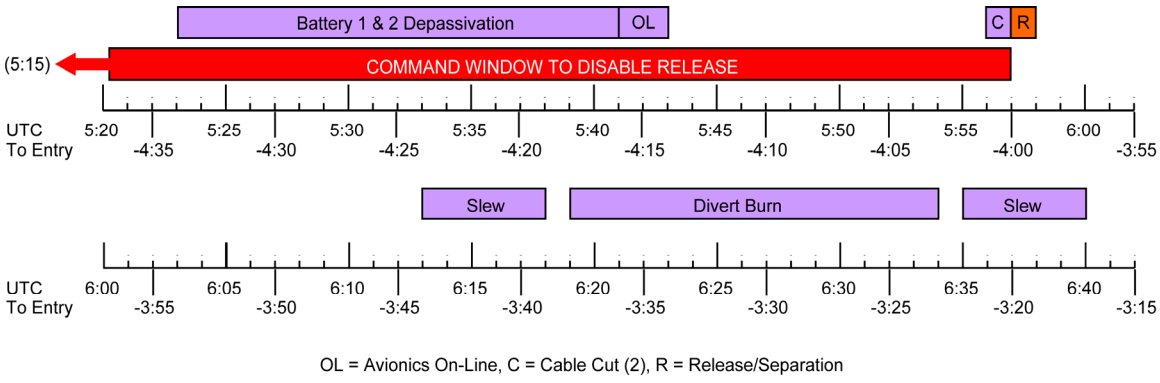



**Figure 1-3. Earth Return Flight Mission Timeline**

primarily to the uncoupled thrusters of the attitude control system (ACS). During safe mode, the ACS would execute unplanned (not forecasted) propulsive activity, which would adversely affect navigation targeting. The last day prior to entry included enabling and executing the SRC release and divert maneuver command sequence. Criteria-based safe-to-proceed ground decisions were made at two points in the operations timeline. A third, autonomous, decision mechanism was implemented on-board the spacecraft using fault protection algorithms and parameter settings.

The SRC release sequence, shown in Figure 1-4, prepared the SRC batteries for SRC free flight by way of depassivation (defined in Chapter 5), placed the electronics on-line with the batteries, cut the electrical connections between the spacecraft and the SRC, and fired separation bolts. A separation spin mechanism provided the separation velocity while simultaneously imparting a stabilizing spin. Roughly 15 minutes after the separation, the spacecraft bus executed the commands to perform a maneuver to divert past Earth. The SRC continued toward Earth on a purely ballistic trajectory and entered Earth's atmosphere 4 hours later. After separation, classified and unclassified Department of Defense tracking systems tracked both the capsule and the spacecraft bus.




OL = Avionics On-Line, C = Cable Cut (2), R = Release/Separation

**Figure 1-4. SRC Release Sequence**

Atmospheric entry occurred when the capsule reached a 125-kilometer (410,000 feet) altitude. Within minutes of reaching this point, radar and other tracking assets at UTTR acquired the incoming SRC. During atmospheric entry, deceleration-sensing switches (G-switches) on board the capsule sensed the deceleration pulse, which started timers that led to the deployment of the SRC's drogue and main parachutes. The timing of these events is illustrated in Figure 1-5.

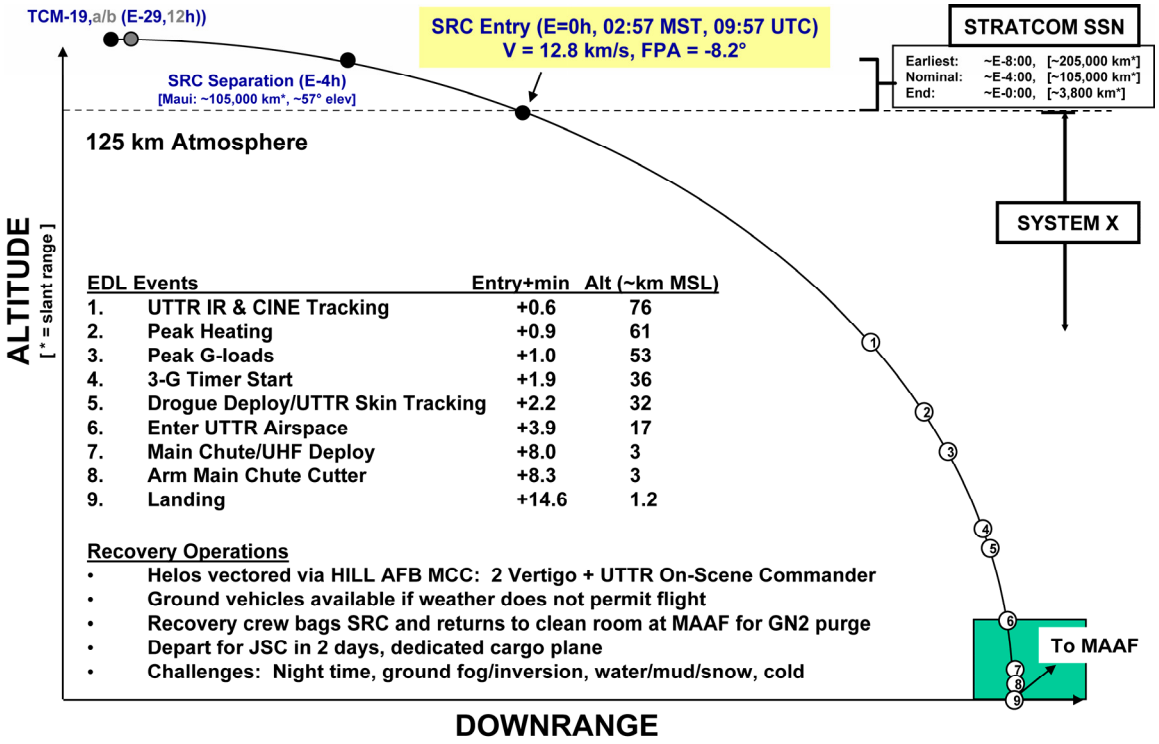



**Figure 1-5. SRC Atmospheric Entry and Recovery**

On the ground, mission controllers at Hill Air Force Base, in Ogden, Utah, vectored recovery personnel, traveling by helicopter, to the SRC. Once the field operations were completed, the SRC was transported back to a clean room at Michael Army Air Field (MAAF) on Dugway Proving Grounds within UTTR where the capsule was opened, and the sample canister, containing the aerogel grid, was processed and packaged for transportation to JSC. The expanse of the recovery area and the landing location of the SRC are illustrated in Figure 1-6.

## Earth Return Preparations

The development of a risk review process at JPL saw its birth within the Mars Exploration Rover (MER) Project, and was carried through to the Genesis Project. The risk effort was largely successful on the MER Project, which is not completely unexpected given the significant resources available. The process on the Genesis Project was somewhat less comprehensive, and as a result proved to be less effective, given a much more limited schedule and constrained funding. The risk assessment process on Genesis was started with only 6 months to go before the Earth return date. A major lesson from the Genesis experience was the need to start the risk process with sufficient schedule to allow mitigations to be put into place, verified, validated, and assessed for residual risk. These processes by which risk was to be identified, assessed, mitigated, and communicated within the chain of command were generated as a result of cultural

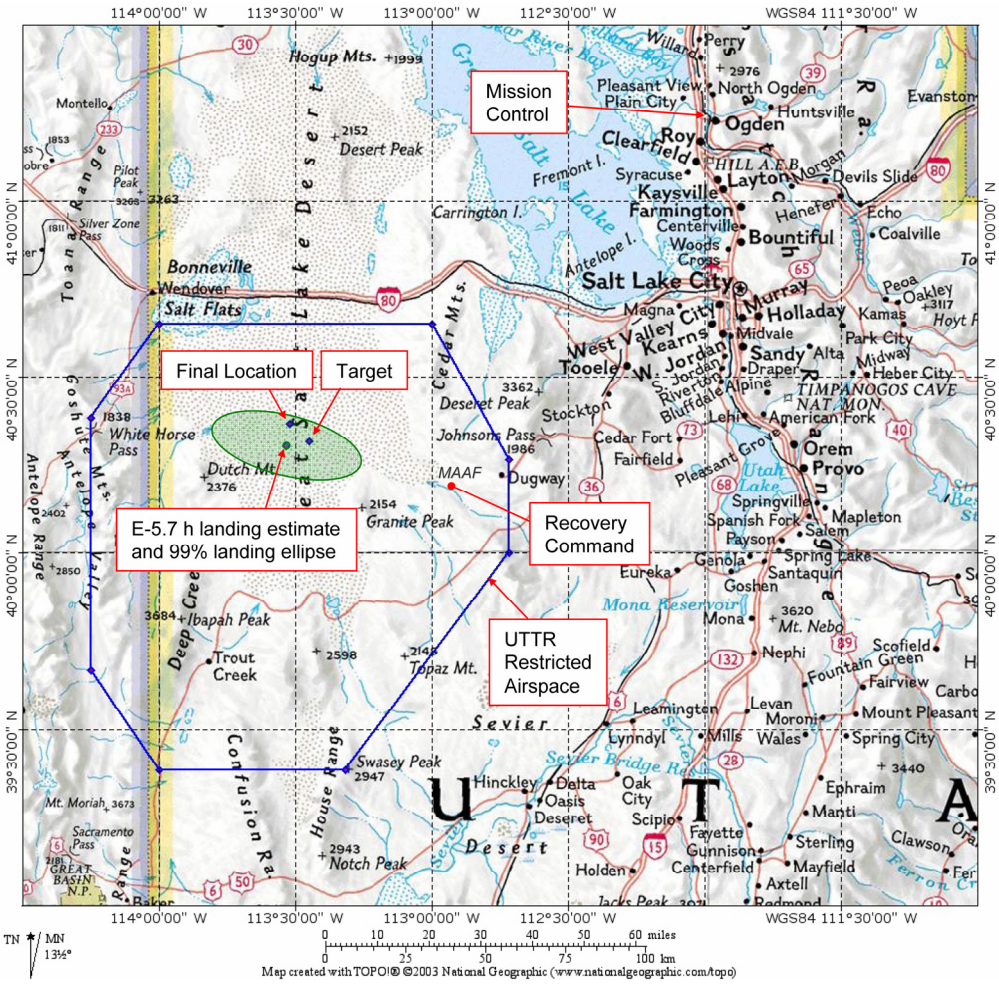



**Figure 1-6. Stardust SRC Landing Location**

changes within the NASA community catalyzed by the publication of the Columbia Accident Investigation Board report [ref 1].

On September 8, 2004, inverted G-switches caused a failure to initiate parachute deployment and resulted in a hard landing of the Genesis SRC at UTTR. The many Earth return mission and technological similarities between the Stardust and Genesis Projects created a need for Stardust to be prepared to respond to the preliminary findings of the Genesis Mishap Investigation Board (MIB). Both spacecraft had been developed during the era of "faster, better, cheaper" missions of the late 1990's and early 2000's. In fact, Stardust was developed almost concurrently with and claimed much heritage from the Mars Climate Orbiter and Mars Polar Lander programs that were subsequently lost in late 1999.

Both Stardust and Genesis were developed under the Discovery program, and with similar partnering structures: NASA Headquarters, Principal Investigator, JPL, and LMSS. LMSS was the industry partner in charge of spacecraft development, spacecraft operations, and recovery operations for both programs. LMSS was also JPL's industry partner for the Mars Climate Orbiter, Mars Polar Lander, and other space programs of the era. In addition, the design of the Genesis SRC was derived from the earlier design of the Stardust capsule, with changes as required by the specific sample capture mechanism accommodation. The Genesis mission profile, however, enabled launch after and Earth return prior to the corresponding Stardust dates. Finally, the Stardust capsule, like the Genesis capsule, was to return to UTTR and the recovery scenario called for a ground landing and recovery, much like the ultimate fate of the Genesis

capsule (recall the Genesis capsule return plan featured a mid-air capture, not a ground recovery).

In January 2005, JPL and Stardust Project management set out to develop a plan that for the final year of operations would be responsive to both the change in the NASA cultural environment and the Genesis mishap. The resulting project plan is illustrated by the review schedule in Figure 1-7. The plan is built around a series of independent reviews that progress from detailed review at the component level (plans, specifications, requirements, and verification and validation) to subsystem peer reviews, followed ultimately by system-level risk and residual risk reviews. Special emphasis was placed on a detailed review of the "as-built" Stardust SRC given the Genesis mishap and a very limited ability to perform in-flight capsule checkouts or modifications.

Essential to this process was the full cooperation of the Genesis MIB chairman, who advocated for and obtained approval to release to the Stardust Project a series of recommendations from the unfinished board report. These recommendations are listed in Table 1-1 and are grouped into two major areas. The first set (FS, Flight System) were those related to the proximate cause of the mishap, the inverted G-switch sensors [ref 2]. The second set (REC, Recovery Operations) were recommendations related to the Genesis Project's operational response to the contingency that presented itself: a hard landing with compromised SRC hardware and threatened sample integrity [ref 3].

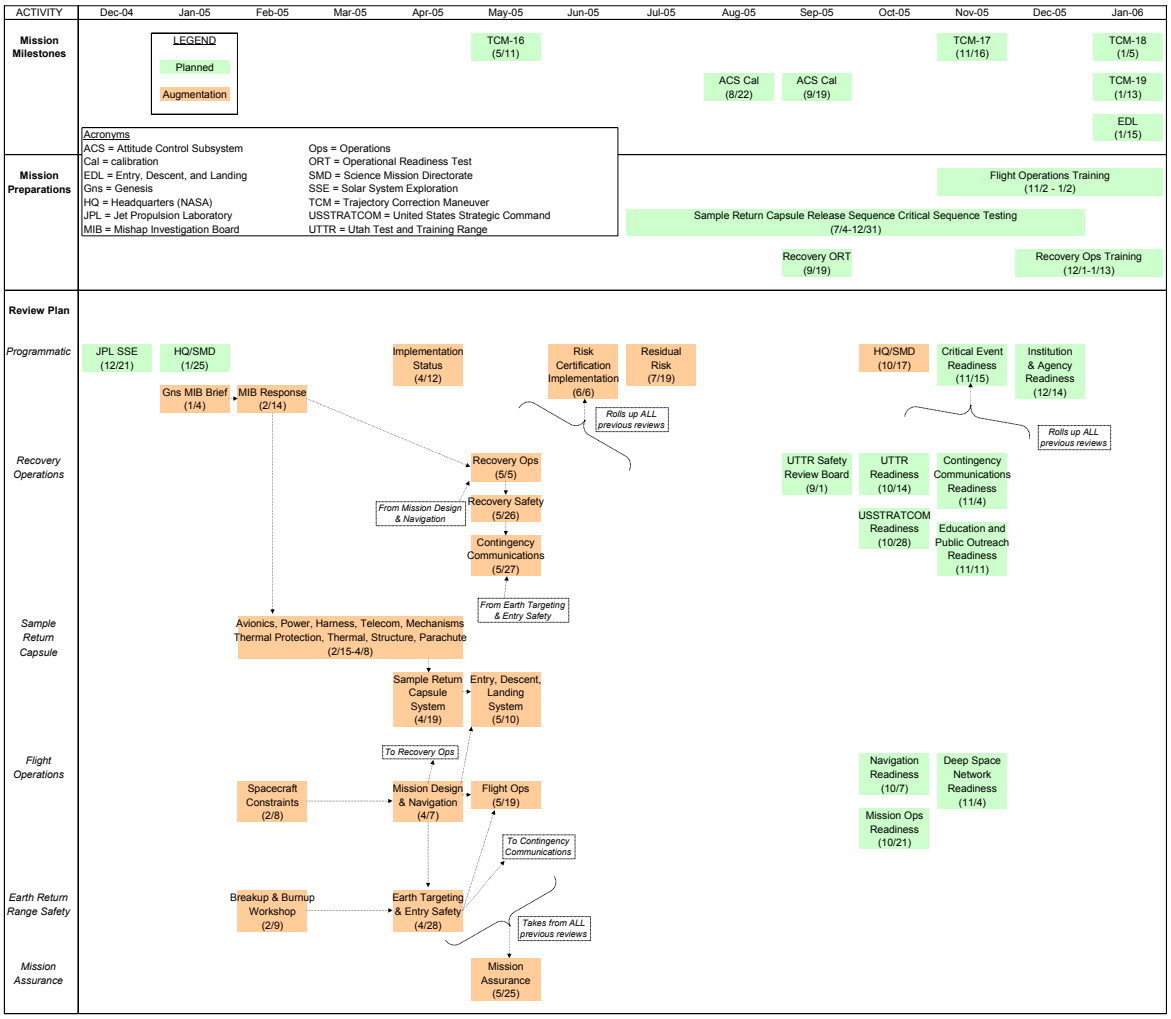



**Figure 1-7. Preliminary Stardust Review Plan and Schedule**

**Table 1-1. Genesis Mishap Investigation Board Recommendations to the Stardust Mission**

| Item | Area |
|---|---|
| 1. Perform destructive physical analysis of the flight G-switch | FS |
| 2. Evaluate effects of G-switch side loads | FS |
| 3. Determine effects of space exposure on parachutes and pyrotechnics | FS |
| 4. Investigate SRC latch operability | FS |
| 5. Determine ablation margin for heatshield and backshell | FS |
| 6. Determine effects of space exposure on seals, vents, and science canister filter | FS |
| 7. Adopt an incident command system process for recovery contingency planning | REC |
| 8. Review recovery contingency scenarios | REC |
| 9. Provide sufficient schedule for recovery contingency review and personnel training | REC |
| 10. Review consistency and adequacy of recovery contingency requirements | REC |
| 11. Assemble a single binder for recovery contingency plans | REC |
| 12. Evaluate Stardust system phasing | FS |
| 13. Review Stardust requirements and verification procedures | FS |
| 14. Review recovery parachute system | FS |
| FS = Flight System, REC = Recovery Operations | |

The Stardust Project's review and preparation plan became a living entity, requiring regular attention and adjustment with the passage of time and execution of events. After some initial start up delays, the bulk of the risk assessment, identification, mitigation, and reporting process was completed in about seven and a half months. The critical event training and readiness certification process overlapped with the risk process and consumed the two and a half months remaining before execution of Earth return events. As would be expected, the latter benefited tremendously from the former in that it allowed the bulk of the technical discussion to be separate, thorough, and to serve as the foundation for the operational plans implemented in the readiness process.

The architecture of the project's plan was simple in its foundation, but somewhat more challenging to implement. Like many (or all) systems engineering efforts, the goal was to comprehensively examine at the subsystem level with an eye toward progressively identifying and addressing crosscutting relationships at the system level. The "as-implemented" review plan is shown in Figure 1-8. The core elements of the project's initial review plan were retained, as required, and in some cases enhanced with additional peer review activity throughout its execution. The mission design and navigation reviews performed in March and April effectively set the baseline mission timeline and environments in which the spacecraft, SRC, and operations teams would be operating. These were followed in mid and late June with a tightly spaced suite of reviews for each of the remaining major elements: SRC system, entry, descent, and landing (EDL) systems, recovery operations, SRC release sequence, and flight operations. The results of these reviews were then all rolled up into the system level Risk, Certification and Implementation review in mid July. Focused residual risk reviews (3) closed out items identified at the system risk review. At the end of this process, the risk was well understood and communicated.

Start up delays, and scheduling constraints, both in personnel availability to perform the required work and efficiency of review board member time commitment, resulted, in several instances, in combining of reviews (recovery safety and recovery operations, and mission assurance and flight operations) and/or less than favorable tight scheduling. As such, the transition from one review to the next was not always serial and the benefits of progressively feeding information and review board feedback from one review to the next were sometimes lost. The loss of serial execution was most evident in the back-to-back execution of the SRC system and EDL system reviews. Originally planned to be conducted with a month of separation, completion of the SRC system review prior to the EDL system review would have allowed for a rolled up, complete list of end-to-end EDL risks to be presented in the latter review. As implemented, the end-to-end assessment was divided between the two efforts, leading to the need for additional coordination and effort to ensure that all elements were indeed being covered.

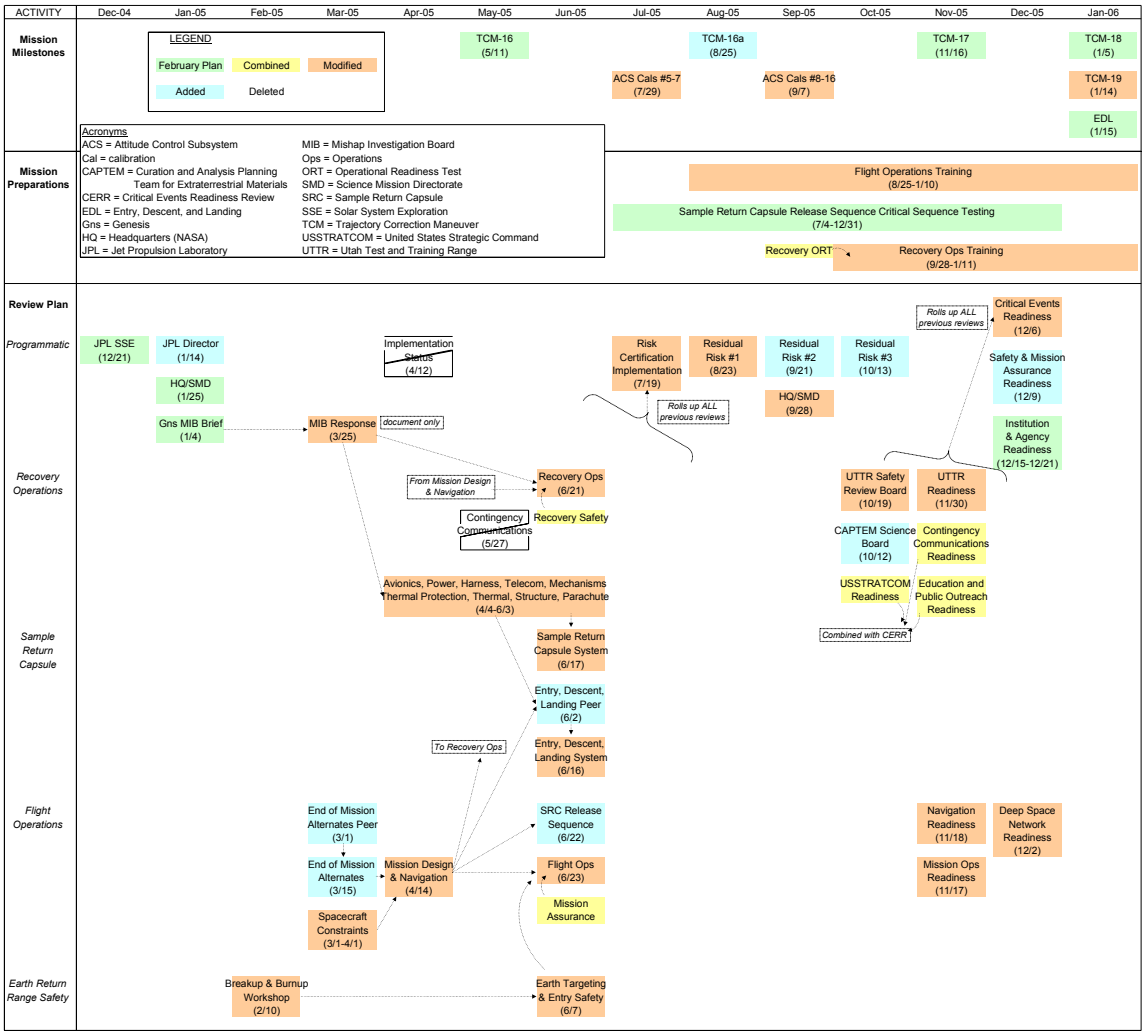



**Figure 1-8. Stardust Review Plan and Schedule As Implemented**

A similar statement can be made about the SRC release sequence review, which was added to the project's review plan within a few weeks of the initial plan release, and the later flight operations review. In this case, however, the back-to-back execution benefited from exceptional information management by the standing review board chairman, who both educated the flight operations review board of the sequence review findings, and kept the flight operations discussion focused on non-sequence issues and system-level interactions. The project's plan would not have been successful had it not been for close, frequent, and open interaction between the lead system engineers at the subsystem (or element), project and review board levels.

The review process did not end with the completion of the risk reviews. Readiness reviews, document approvals, and procedure approvals, in parallel with test and training efforts, were quick to follow, including the development of a Certificate of Critical Event Readiness (described further in Chapter 8). In an attempt to improve review efficiency, several subsystem readiness reviews were combined with the project level Critical Events Readiness Review; this was not done with the critical Navigation and UTTR readiness portions. In addition, the criticality of the Earth return event warranted an independent Safety and Mission Assurance Readiness Review conducted directly with NASA's Office of Safety and Mission Assurance. Higher-level briefings with JPL, LMSS and NASA Headquarters upper management completed the readiness review process and ensured proper communication of the project's risk and readiness posture.

## Project Organization

The Stardust Project's organization was necessarily expanded during the execution of the risk and readiness activity and is illustrated in Figure 1-9, with those elements added to the organization clearly designated. Beyond the external partnerships required to execute the recovery event, subsystem and systems engineering support was added to address several specific areas of concern. Beneficial to the overall success of the project's plans was the addition of lead system engineers who worked on the Genesis mission and who were familiar, not only with the risk process implemented therein, but, also, with the ground-breaking development of the required Earth return range safety analyses, and operational criteria, and the elements of the recovery operations on Genesis that were the subject of MIB attention.

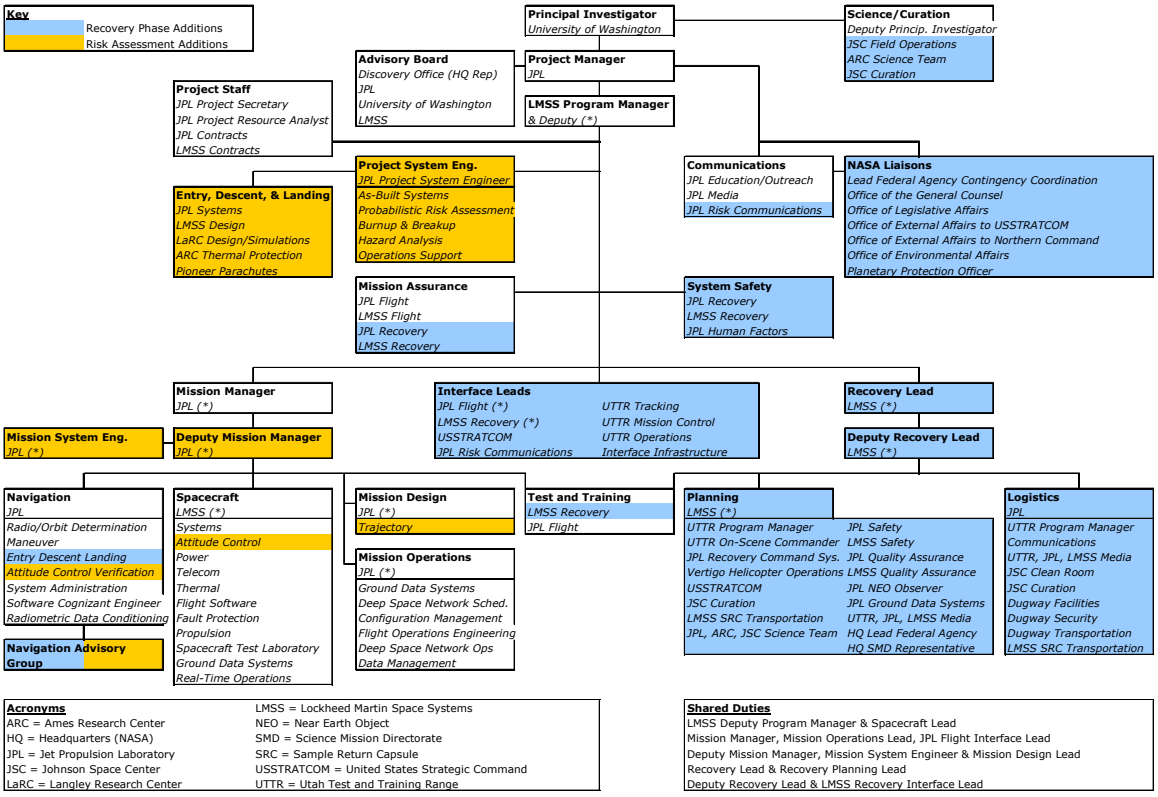



**Figure 1-9. Stardust Project Recovery Preparations Organization**

Navigation and attitude control support was expanded to ensure the SRC was properly targeted to the desired location at UTTR. Hardware experts, in particular electronics experts, were brought on board to examine the SRC design, fabrication and requirements validation. EDL analysts and system engineers were tasked with end-to-end risk evaluation of flight dynamics and loads with particular focus on performance of the thermal protection and parachute systems.

One particular workforce challenge was a suggestion by senior management to form two independent teams within the project organization – one dedicated to flying the mission, and one to focus on the critical event preparation. It goes without saying that this comment applied primarily to the flight operations teams, including navigation. Recovery, SRC experts, and EDL experts were able to completely focus on the assessment and preparations tasks, unhindered by day-to-day operations. The flight operations team split was accomplished with limited success and was applied primarily at the middle-management level (Mission Manager, Project System Engineer, lead engineers at LMSS). Further division of labor was very loosely enforced and

delegated to the team lead and analyst level. The benefit of this approach was that it allowed the team leads and analysts to retain management responsibilities for division of labor and, perhaps more importantly, it allowed for efficient collaboration and cross-training between the development task and flight experience.

## The Balance of the Primer

The remainder of the main body of this document is organized in ten chapters that describe, in more detail, the risk and readiness activities conducted by each major project element in as general a manner as possible, but using the Stardust specific scenarios as examples and illustrations. Together they describe what was done, why it was done, and whether it worked. Several appendices follow the main body of the document. The appendices contain a more classic set of element-by-element, Stardust specific, lessons learned and a few observations beyond the Stardust experience. The final appendix is a table of contents of all of the Stardust review material, review board reports, and project documentation produced during the final year of operations. That material is contained in a compact disc that accompanies this document.

Chapter 2 describes the mission design and navigation preparation effort, which had the primary objective of delivering the SRC to Earth's atmosphere within the required tolerance to survive entry and arrive within the designated landing area. The navigation strategy was responsive to Earth return safety compliance, dominant error sources and targeting sensitivities, and was robust to the perturbations resulting from credible contingency scenarios (e.g. safe mode entries that resulted in unplanned propulsive activity). The discovery of a disagreement between the attitude control and navigation analysts over error modeling and the subsequent re-certification effort is also described in this chapter. Finally, the chapter discusses readiness preparations, which were comprised of the development, test and training, and certification of operations procedures, staffing plans, software tools, hardware and facilities.

Chapter 3 provides the step-by-step recipe and challenges encountered in the development of the project's compliance with Earth return range safety requirements essential for sample return. Starting with the characterization of the entry trajectory, determination of skip out conditions and the progression of the instantaneous impact track, the effort proceeded through several independent breakup and burnup analyses, calculation of possible debris ellipses, and concluded with independent population and property hazard analyses. Also described are the advantages of avoiding population centers, which enabled the use of easily defendable spacecraft reliability arguments, and the challenges resulting from the lack of real-world data for in-depth verification and validation of breakup and burnup analyses of small, SRC sized, entry vehicles.

Chapter 4 describes the development of the entry decision criteria that ensured compliance with Earth return range safety requirements during the actual return operations. The development of a comprehensive and thorough project-wide decision timeline and flowchart set the overall system context for the development of criteria details. This was followed by the systematic assessment of the need for and development of the SRC release enable (green button), the SRC release disable (red button), and spacecraft divert disable (purple button), each of which considered contributions from navigation, the spacecraft, and mission operations. In addition, the implementation of the decision criteria carried with it a proper understanding of data flow to the decision makers, and certification of supporting software and hardware. The important role of test and training in the validation of the decision criteria is illustrated by the discovery of several omissions and errors during operational readiness tests.

Chapter 5 summarizes the activities performed to identify and characterize the hardware risks related to the Stardust SRC. Prompted by the Genesis mishap and the dormant nature of the capsule (for 7 years), the review effort relied heavily on the examination of pre-launch specifications, schematics, and verification and validation records. With not every subsystem contributing to the success of the EDL operation, the chapter describes the prioritization of the

review effort and eventual binning into three distinct categories depending on their potential contribution to return operations planning and return risk knowledge. Also described are the challenges associated with flight spare testing of G-switches performed to compare with pre-launch results and achieve independent verification and validation of functionality.

Chapter 6, in similar fashion to the SRC review effort, captures the identification and characterization of the end-to-end EDL system. Using a success tree methodology developed for MER and applied on the risk assessment for the Cassini mission's Huygens probe, the chapter describes the activities performed to examine overall entry systems, simulation and flight dynamics, avionics (with some minimal overlap with the capsule review process), parachutes, aerothermal analyses, and the design of the thermal protection system. The last of these was of particular importance for Stardust as it was the first flight of a phenolic impregnated carbon ablator. To take advantage of capabilities beyond requirements, the re-certification effort for a wider entry flight path angle error in support of the entry decision criteria development is also described in this chapter.

Chapter 7 contains the preparation efforts required to integrate the navigation strategies, decision criteria, and SRC separation sequence into one seamless mission, spacecraft, and ground data system operations construct with proper interface support to non-flight components, i.e. it describes the flight operations preparation process. In addition to the risk and readiness processes that concluded with the certification, through test and training, of hardware, software, personnel, operational procedures, interfaces, and staffing plans, the chapter describes the characterization of the spacecraft performance required for the return operation and the development, verification and validation of the SRC critical command sequence.

Chapter 8 describes the roles and responsibilities of the flight operations assurance effort and the importance of providing an independent perspective to the risk assessment and readiness processes. Functioning, for the most part, in parallel with the mainline project effort, described in this chapter are the institutional and project wells that were tapped to ensure the project properly considered its development and flight history, and kept on track with institutional expectations.

Chapter 9 provides a very important and essential guide to the interactions between the project and supporting external organizations. Described are the suite of support agreement documents required many months prior to the actual return event, followed by the operational interface agreements and infrastructure that ensured successful data transfer and voice communications. The key organizational interfaces contained within the chapter's pages are primarily between the flight operations teams and United States Strategic Command, mission control at Hill Air Force Base, and recovery command at Dugway Proving Grounds. Additional text describes the required plans, scripts, interfaces and contacts between recovery command, NASA HQ and other federal agencies, which would have been needed in the event of an anomalous entry.

Chapter 10 is one of the more valuable parts of this document in that it describes the planning and training activities required to ensure that ground teams were prepared, with the aid of a recovery command system, for every credible sample recovery scenario. The suite of preparations encompassed integrated nominal and contingency operations plans, procedures and interfaces, safety plans and manuals, training plans and certification logs, and selection and calibration of scenario dependent hardware. These preparations always ensured that human safety was properly prioritized over mission success.

Chapter 11, the final primer chapter, describes the roles and responsibilities of the independent recovery safety effort. Contained within the chapter is the story of how the single person effort tasked with independent identification and characterization of recovery safety hazards and evaluation of operations compliance with institutional and agency safety requirements was expanded to include a several member, multi-disciplinary Independent Review Team to comprehensively and thoroughly fulfill the task charter.

Enjoy!

# Chapter 2: Mission Design and Navigation

Achieving delivery of a sample return capsule (SRC) to a relatively small location on Earth is a challenging but feasible task. For Stardust, an illustrative comparison, like the ones popular with the media, was that the predicted delivery accuracy to the Earth's atmosphere was the equivalent of a baseball pitcher throwing a strike from about 64 kilometers (40 miles) away, given a strike zone defined by the batter's knees and chest. The final targeting maneuver, which was implemented at 29 hours from entry, delivered the capsule to within a kilometer of the intended target in the B-plane (a representative vertical plane at perigee) or within a few inches of the center of the strike zone.

Mission design and navigation were crucial to the success of the Stardust Earth return, serving as one of the main tributaries feeding the project's operational planning and risk assessment. The baseline design provided the timeline around which operations would need to plan, defined the conditions under which the capsule was delivered to the atmosphere, and, ultimately, provided the landing ellipses, nominal and off-nominal, that were used for range safety assessments and recovery operations planning.

This chapter describes the tasks and challenges encountered during the development of these fundamental building blocks. It is the first subsystem specific chapter because the preparation efforts described in subsequent chapters required results from the mission design and navigation efforts to complete their preparation activities. In addition to the developments required for planning purposes, this chapter also describes the tasks completed by the navigation team to prepare for their participation in the operational phase of the Earth return.

## Defining the Mission Baseline

The primary objective of the mission design and navigation strategies was to target the SRC with an accuracy that would ensure its survival through the atmosphere, as defined primarily by entry flight path angle constraints, and a landing within the approved regions of the Utah Test and Training Range (UTTR). If that were not challenging enough, the strategy also needed to be compliant with range safety requirements (Chapters 3 and 4), recognize dominant error sources, fit within spacecraft constraints, and be robust to credible contingencies.

Navigation in space requires detailed models of forces acting on the spacecraft, including gravitational forces produced by various bodies, solar radiation pressure, and outgassing and thrusting of the spacecraft itself. These models are calibrated to predict the future position and velocity of the spacecraft, and to determine corrections required to keep it on course, per the mission design or plan, developed in advance [ref S3]. Deep space navigation utilizes the antennas of the Deep Space Network (DSN), located at three sites around the world (Goldstone, California; Canberra, Australia; Madrid, Spain), together with on-board systems, in particular telecom, attitude control, and propulsion, to gather the data required for the state estimation and to execute the calculated corrections. Earth return navigation involved three specific sub-disciplines: orbit determination, maneuver design, and entry, descent, and landing (EDL).

Orbit determination was concerned with determining the trajectory state (position and velocity) of the spacecraft at various times, based largely on radiometric tracking data from the DSN, and force and measurement models. One model important to Stardust, small forces, consisted of a history of the effects of thrusting events via the spacecraft telemetry, and predicted thrusting behavior extending into the future. All such data were fed into a mathematical filter, which provided the best possible estimate of future spacecraft states. Such data also included a model of the separation of the SRC from the main body of the spacecraft [ref 14].

Errors in orbit determination, modeling of spacecraft performance, and unexpected events or anomalies could result in the spacecraft deviating from the planned or nominal trajectory. The maneuver design discipline would use the state solutions provided by orbit determination to calculate course corrections, commonly known as trajectory correction maneuvers (TCMs), to force a return to the nominal trajectory as defined by the mission design. Most maneuvers for Earth return were targeted through future events to a state at the entry interface point, located at a geocentric altitude of 125 kilometers (410,000 feet) and just outside of the Earth's atmosphere. The final TCM would be targeted directly to a location on the ground to ensure a full understanding of end-to-end targeting sensitivities [ref 10].

The EDL discipline specialized in simulation of the trajectory and attitude of the capsule during atmospheric entry based on detailed models of the Earth's atmosphere and the aerodynamic, aerothermal and parachute deployment characteristics of the capsule. They supported maneuver design strategies in the development of targeting directly from space to the ground and range safety analyses with landing ellipse and/or debris ellipse predictions as a function of mission event (see Chapter 3 for more detail). In addition, supported by post-TCM trajectory reconstruction performed by orbit determination, their landing location estimates were used in the capsule release decision processes (Chapter 4). Finally, their work would also aid pre-deployment of recovery assets and initial pointing of entry tracking assets (visual, infra-red, and radar) (Chapter 10) [ref 11-13].

The navigation strategy for Earth return evolved significantly from pre-launch and early flight operations. The navigation team began tackling many of the Earth return details in late 2002 and early 2003, prior to the Wild 2 comet encounter. These details included introduction of maneuver biasing, as well as in-fight calibrations, which will be explained later in this chapter. The addition of the risk assessment process would create more in-depth examination of the existing Earth return strategies, further characterization of the navigation and spacecraft systems, and refinement of navigation strategies. This process, as described in Chapter 1, consisted of a series of focused reviews, the general goal of which were to identify and, if possible, mitigate risks in achieving a safe and successful return of dust samples collected by Stardust.

Before any significant work force was expended in the detailed examination of the navigation strategies, the Stardust Project set out on a mission design trade study of alternate endings to the mission. Prompted by the Genesis landing mishap, the primary reason for the trade study was to examine the possibility of changing the landing time from the baseline nighttime (3 am local) to daytime with the expectation that it would be better for recovery operations in the event of a similar outcome. In addition, contrary to Genesis, the Stardust baseline mission did not have an option for a backup return opportunity, so it was also investigated. And finally, there was a desire to examine the feasibility of a follow-on mission for the spacecraft bus, following completion of its primary mission. Daylight, backup orbit, and follow-on mission trajectories were developed and reviewed at the End of Mission Alternates review. The completeness of the trade study is illustrated in Figure 8-4 given the role played by mission operations assurance in the assessment of the trade. However, the daylight option was abandoned primarily for two reasons.

The first was that the dayside entry would require a retrograde entry and a correspondingly higher Earth relative entry velocity. Although there was a preponderance of trade elements that were leading the project to abandon the daylight entry, this by itself was sufficient for many of the external reviewers, almost leading to an abrupt end to the review. The reduction of heatshield margins resulting from a retrograde entry, compared to a posigrade entry, was deemed too risky given this was the first flight of the SRC's thermal protection system even though the detailed risk examination of the SRC systems (Chapter 5) and EDL (Chapter 6) had not been completed at this juncture of the preparation effort.

The second detrimental characteristic of the daylight entry was that it moved the trajectory's potential debris track from south of Salt Lake City to cutting directly through Salt Lake City, significantly raising the difficulty of achieving range safety compliance (see Chapter 3 for more

detail). Finally, in so far as the primary objective of aiding recovery operations contingency planning, the value of a daylight entry was not deemed high enough to outweigh the risk of the capsule's survival of EDL. In addition, there was some disagreement of whether it was better to be marching toward daylight or marching toward nighttime in the event of an anomaly. As for the other objectives of the review, the project did adopt a 4-year backup orbit (more on this in Chapter 7), but abandoned the post-mission follow-on opportunities due to a higher than desirable cost in propellant margin. This review, which effectively confirmed the trajectory baseline, encompassed the bulk of the mission design preparation effort.

The navigation designs for the baseline mission were the topics of the Mission Design and Navigation Peer review held in April 2005. One of the main topics was the strategy for placement and implementation of the final TCM, based on the navigation requirements and spacecraft performance characteristics, which themselves were based on in-flight calibrations and flight history. To that end, the primary finding from the review was that the project needed to place more emphasis on understanding and characterizing all navigation error sources, in particular for maneuver execution, to achieve concurrence across teams regarding the results derived from in-flight calibrations performed in 2003. In addition, the board supported plans to proceed with follow-on calibrations later in the year. Such improvements in knowledge would provide the basis for refining the placement of the final pre-entry maneuver. Further detail on these topics is provided later in the chapter. Additional review findings called for improvements to tools to more accurately assess ground dispersions resulting from the planned maneuver implementation (fixed direction), independent verification of the velocity imparted by the capsule separation, and further definition of criteria for implementing or canceling maneuvers as a function of anomalous activity.

The refinements in the navigation strategies were presented as part of the Flight Operations review that was held in June 2005. However, assumptions about the validity of execution errors, based on in-flight calibrations and flight history alone, were called into question due to the limited number of samples being used in the analysis. A request was made for the project to develop and implement a maneuver error certification process that would lead, primarily, to a comprehensive set of execution errors endorsed by both the navigation team and attitude control subsystem personnel. The certification process was completed in time for the third Residual Risk review held in October 2005 and is discussed in more detail later in this chapter.

Overlapping with the conclusion of the risk review process, the navigation effort turned to preparing for operational support of the Earth return activity. Readiness to support operations would encompass review, and development, as needed, of procedures and interfaces, software tools, hardware infrastructure, staffing plans and duty rosters, and participation in the project's test and training program. Particular attention would be paid to developments required to support targeting directly from space to the ground (navigation and EDL software interfaces), Earth return range safety analysis (see Chapter 3), maneuver and capsule release decision criteria (see Chapter 4 for a specific trade study conducted on whether to develop new software versus a manual process in support of part of the decision criteria evaluation), EDL simulations, and interfaces with external agencies (Chapter 9). A navigation-centric operational readiness review was held with JPL institutional navigation experts, known as the Navigation Advisory Group, in November 2005, as a prelude to the project's Critical Events Readiness Review. These reviews focused on the outcome of the operations preparations efforts, including lessons learned from participation in the test and training program.

## Selective Key Preparation Topics

The previous section provided the general components of the mission design and navigation preparation efforts. This section provides selective additional detail for several efforts that required special attention. While somewhat Stardust specific, they provide examples of the importance of characterizing spacecraft behavior, certifying that behavior for use in operations,

and application of said knowledge in the baseline and contingency planning of the sample return navigation strategy.

### *Spacecraft Performance and Maneuver Biasing*

Stardust employed a three-axis attitude control system (ACS) with uncoupled or unbalanced thrusters and without momentum wheels. Thus, the attitude control function produced changes in velocity, which affected the spacecraft trajectory and targeting to Earth entry. The suite of propulsive activities for Stardust included limit cycling (maintenance of attitude within prescribed angular deadbands and rates), turns (or attitude maneuvers) associated with maneuvers, Earth communications, and calibrations, and burns associated with the maneuvers themselves.

The assumptions used for Earth return analysis and planning evolved significantly over time. Prior to launch, the required entry flight path angle could be achieved with the maneuver execution errors (fixed and proportional) found in project requirements documents. Unfortunately, after the execution of several maneuvers in flight, it was evident that execution errors were driven by the turn components of the maneuvers and were much larger than expected, usually by an order of magnitude. This discrepancy was linked to the inability of the ACS controller algorithm to compensate for uncertainties in the spacecraft's center of mass resulting from the position of fuel mass within the propellant tank (more on this specific topic in Appendix G). This effect could not be eliminated in flight, but was mitigated in two ways: fixed direction maneuvers, and slower turns for maneuvers. The first eliminated the turn error completely and was implemented for the final TCM. The second, implemented at the penultimate maneuver, kept the fuel mass relatively stationary during turns in support of the maneuver, allowing the algorithm to compensate. However, since the turn was slower, the maneuver took longer to execute, and introduced direction constraints due to solar power availability and spacecraft battery capacity.

Originally, maneuvers associated with the Earth entry phase were entirely statistical [ref 4], having nearly uniform likelihood of requiring a velocity change in any direction. Deterministic biasing of maneuvers was introduced into the reference trajectory (that is the trajectory design was modified to include a required change in velocity at the designated maneuver epochs) as the solution for limiting or eliminating the need to turn the spacecraft, thus minimizing the maneuver execution error. These biases were found to be required at the final two maneuver epochs in order to achieve the required entry conditions. The direction of the biasing was selected to be either sunward or along the prevailing attitude of the spacecraft as established by the attitude plan.

Such biasing also had a side benefit of enhancing ground safety in the event of a catastrophic failure during Earth approach, as indicated in Figure 2-1. In other words, failure to execute the now-required entry maneuvers would generally have the effect of causing the spacecraft, with the sample capsule attached, to safely fly by the Earth in accordance with range safety requirements.

### *In-Flight Calibrations and Execution Error Certification*

In order to reduce targeting error and maximize predictability of all propulsive events, in-flight calibrations were performed on Stardust beginning in 2003. The calibration activity encompassed spacecraft limit cycling, deadband walks (or slow turns), and maneuvers with the goal of identifying sources of systematic error and better characterization of the spacecraft's attitude control behavior [refs 5-8]. Characterization of limit cycling behavior was of great importance for Earth return, where the solar distance approached 1 astronomical unit (AU), since the velocity change resulting from said behavior was not directly controlled, i.e. the spacecraft attitude and deadband limits were driven by other planning requirements and the resultant thruster activity was a by-product of that selection and the flight environment (e.g. solar radiation pressure). That being said, tighter deadband limits were generally believed to produce more predictable behavior (more on that later in this chapter). The calibration would improve the predictability of this limit cycle behavior and allow for its inclusion in maneuver design.

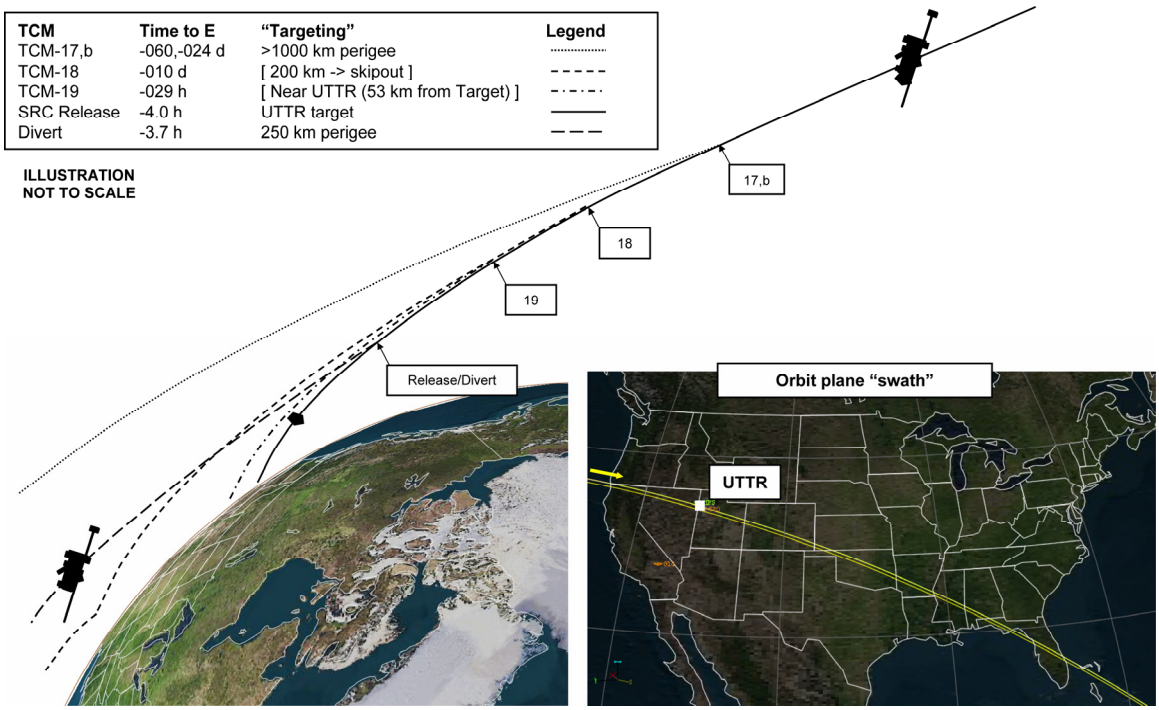



**Figure 2-1. Earth Approach Navigation**

The initial set of Earth return calibrations were executed in the summer of 2003 to take advantage of a period of the mission where the solar distance reached a minimum of 1 AU and attitude control behavior was influenced by solar radiation pressure that was similar to that of Earth return. The 2003 calibrations provided results pertaining to limit cycling at the capsule release attitude and deadband setting, a limited set of deadband walks, and the existing maneuver execution sequence. The navigation and spacecraft teams, in particular attitude control, interacted extensively in the planning, execution and analysis of the calibrations. The effort led to a proposed redefinition of the maneuver sequence that would remove systematic errors resulting from attitude drift between maneuver piece-parts. The team interaction also led to the desire to repeat and expand the calibrations at the next available opportunity. With emphasis shifting to the upcoming comet encounter (January 2004), further calibration activity was deferred.

Increased interest in further in-flight calibration and characterization of the spacecraft's performance occurred as a result of the risk identification and mitigation processes put into place during the final year of preparation for Earth return. Calibration plans for the latter half of 2005 and results from the earlier 2003 calibrations were reviewed over the course of the ensuing review process. The errors derived from the limited 2003 sample set, in addition to expected improvements in the maneuver execution sequence, were presented at the Flight Operations review in June 2005. The review was attended by several attitude control analysts that had been away from the Stardust Project since launch, who questioned the execution error assumptions being made by the current flight team based on their experience with pre-launch requirements validation work. In addition, the review board questioned the validity of using a limited sample set as the sole source for determining execution errors. The interaction at this review led to the request for a maneuver error certification effort, as mentioned earlier in this chapter.

An essential initial ingredient to the certification effort was to achieve concurrence on the definition of execution error, or said more plainly, to make a list of all of the sources that contributed to the total error in the execution of a maneuver. It was additionally important to identify which of these sources comprised the bulk of the error with the goal of focusing analysis and calibration on those sources. Though it may seem odd that achieving this concurrence would be required on a project with as much flight time as Stardust, the disconnect was left over from

pre-launch requirements development and was never amended due to fairly loose navigation accuracy requirements for the mission up until the return leg. In the pre-launch documentation, maneuver error requirements had been established and verified assuming the requirement statement applied only to the main burn component of the maneuver execution. The navigation interpretation of the requirement, however, had been that the requirements statement encompassed all error sources, turns and the main burn. Prior to proceeding with the Earth return certification task, the navigation and spacecraft teams agreed to a proper definition of the execution error.

The maneuver error certification effort was constructed to consider two sources of information: in-flight calibration data and attitude control Monte Carlo simulations. Even though the in-flight calibration plan was augmented during the Earth return leg, there would only be 4 to 10 calibration samples for any particular attitude control function. The calibration data would end up having extremely good consistency, and smaller execution errors than the pre-launch requirements and Monte Carlo simulations, but its sole use in the definition of execution errors was confirmed to be statistically unsound upon application of statistical methods for small number of samples (e.g. chi-squared analysis). As a result, the maneuver errors that were certified for operational planning were based primarily on updated simulations of the attitude control performance. The Monte Carlo approach provided large sample sets, and, with the update to current spacecraft characteristics, produced errors that were smaller than the pre-launch requirement, just not as small as suggested by the in-flight calibrations. It was conceded, however, that the simulations provided rather conservative error bounds, which was somewhat confirmed by the in-flight calibration results (and demonstrated the value of having performed the in-flight calibrations).

***Significant Maneuver Modifications and Contingencies***

The results of the maneuver error certification effort were used to establish the desired time of the final TCM as 36 hours from entry to ensure delivery of the capsule within the atmospheric entry requirements. Operational considerations, such as overlapping DSN antenna coverage and improved regularity in duty rosters, would result in that final maneuver being moved to 29 hours from entry. A contingency maneuver opportunity was placed at 12 hours to protect against a failure to execute the primary opportunity, which was essential given the need to remove the deterministic bias that had been added to the trajectory. But, why these maneuver epochs?

The risk balance equation for the terminal navigation approach was quite complicated given the unbalanced thrusters in the attitude control system and the biased maneuver strategy. It was highly desirable to complete navigation targeting of the critical event as far out from entry as possible to provide time to respond to low-probability contingencies. The selection of 29 hours for the final targeting maneuver on Stardust was close to the earliest possible while still meeting entry requirements. However, the accuracy of the navigation strategy depended highly on the predictability of future propulsive activity, in particular following the start of the design process for the final targeting maneuver. Unplanned propulsive activity could alter the navigation targeting, the effect being larger with greater time from entry.

The leading candidate for an anomaly during the Stardust return phase was a solar event that would place the spacecraft into safe mode. If the safe mode occurred during execution of the final baseline maneuver there would be a failure to remove the trajectory bias and the estimated landing location would fall short of the desired target. On the other hand, a safe mode entry that occurred during a 8-10 hour window after the completion of the final maneuver, due to its effect on the attitude control system, would impart additional, unplanned and, therefore, unpredicted velocity change and would move the estimated landing location beyond the desired target. Sensitivity analyses had determined that safe mode entries, when occurring earlier than 20 hours from entry, produced sufficient velocity change to move the targeted landing location outside the approved landing zone. Both of these safe mode scenarios changed the predicted velocity profile such that the required landing location would not be achieved.

The response to the first anomaly was relatively benign assuming, of course, that the anomaly had not affected the ability to perform a maneuver, which was certainly one of the contingency maneuver execution criteria. The contingency maneuver would be in the same direction as the baseline, and, as a result, would be as accurate. The overall project risk was relatively low from selecting this response option for this scenario. Execution of the contingency maneuver in response to the second anomaly, which was one of the higher risks to the navigation strategy, required the maneuver to be performed in the non-preferential direction (one requiring large, error-prone spacecraft turns); a direction that provided only a 70-80% chance of successfully targeting back within the desired landing area. The closer the contingency maneuver epoch could be to the entry epoch, the smaller the effect of the large execution errors on the resultant navigation delivery. The placement of the contingency maneuver epoch at 12 hours was a balance between delaying execution and still allowing sufficient time for maneuver reconstruction in support of the capsule release decision processes.

## Preparation Challenges

Beyond the mainline mission design and navigation efforts, there were several, smaller challenges, that affected preparation planning and execution. They are captured below as they encompassed some of the interesting debates and ancillary lessons learned during the preparation effort.

### *To Calibrate or To Improve?*

During the planning and execution of the spacecraft calibration activities, standard operating procedures came to be in conflict with the goals of the calibration effort. It had been the practice of the attitude control analysts to update mass properties and corresponding algorithm parameters in an effort to periodically match the spacecraft state and optimize algorithm performance. A debate arose as to whether it was better to continue to improve spacecraft performance or improve the knowledge of spacecraft performance. Given the concerns already expressed about the small size of the calibration sample set, the decision was made to preserve and maximize the integrity of the calibrations by halting the trending and improvement effort, effectively freezing the configuration of the attitude control algorithm. However, care was taken to ensure that the calibrated results would not become invalid by the time of the Earth return. The remaining flight events were examined for any that would result in large changes to the spacecraft state. Aside from the capsule release itself, there were none.

### *Engineering Judgment: Deadband Selection*

Careful consideration was given to the Earth approach attitude plan given the importance of being able to accurately predict the velocity changes imparted by the attitude control system. A configuration with tight deadband limits, maintained over a relatively long period of time, was thought to have the benefit of maximizing the predictability of thruster behavior as thruster torques would invariably overwhelm solar radiation torque.

The drawback of very tight deadbands, as would be required for the capsule release event, and also the ones deemed most predictable, was that they required use of the inertial measurement unit (IMU) for accurate attitude maintenance. Relatively large deadband settings had been used for the bulk of the mission since they did not require use of the IMU, and conserved IMU lifetime. These large deadband settings were found to be one-sided; solar torque effects dominated thruster torques. In addition, the attitude behavior and velocity production from a one-sided deadbanding configuration, or, for that matter, changes to deadband settings, in particular tightening, was difficult to predict due to the randomness of the starting point within the deadband box.

For these reasons, the tight deadbands that were to be used for the capsule release event were selected for use for the entire month preceding capsule release. Unfortunately, this selection was primarily judgment based as the calibration activities performed in support of spacecraft characterization were insufficient, or, more accurately, insufficiently analyzed early enough, to confirm the behavior expectations of the tight deadbanding. In reality, the tighter deadband configuration only served to eliminate the need to estimate the velocity imparted by changing deadband settings, but did not eliminate the randomness of the behavior. The ability to predict one-sided versus two-sided deadbanding behavior remained elusive through the final navigation targeting and capsule release [ref 7]. Ultimately, the navigation delivery accuracies were met by adopting aggressive and dedicated trending procedures that then fed back into the terminal maneuver designs.

***Failure to Decompose? Target out of the Box!***

Late in the test and training program, the test gremlins devised a scenario that required implementation of the 12-hour contingency maneuver with large turns. The safe mode entry had occurred with a magnitude and a time that placed the estimated landing location uncomfortably near that which was unacceptable. It was sufficiently close that the contingency maneuver design process was initiated. The decision on whether the maneuver would be implemented would come at the conclusion of the design process with the aid of additional navigation tracking data, which would be used to confirm the previous landing location result.

The test exercise encountered an unexpected twist when maneuver decomposition software failed to decompose the very small maneuver size into its constituent turn and burn components. The failure was traced to the aggregate turn components being larger in magnitude than the total requested maneuver size given the unbalanced thruster configuration of the spacecraft. The solution to this class of failure was well known within navigation and attitude control circles, which was to force the maneuver turns to complete a full 360° complement, thus removing the turn contribution from the desired velocity change. The existing, tried and true, Stardust maneuver implementation established turn direction based on the minimum turn size between the initial attitude and the required main burn direction. For the bulk of the mission, and for most maneuver sizes anticipated during the Earth return, the existing implementation was perfectly acceptable.

Should the project implement changes to the maneuver implementation process for this low probability contingency, particularly this late in the readiness preparation process? Out of the box thinking found an alternate solution to the decomposition problem. Instead of changing the maneuver implementation, an alternate landing site could be targeted, forcing an increase in the size of the contingency maneuver, beyond that where decomposition algorithms would fail. The alternate landing site was still well within the approved landing area.

## Successful Outcome

Many on the navigation team had experienced the initial disappointment of the drogue parachute deployment failure on Genesis, which obscured the outstanding effort and result achieved by the navigation strategies implemented on that mission. Like Genesis, the navigation delivery of the Stardust capsule to the atmosphere was dead-on and ground sensors, including cameras, were able to lock on to the heat signature of the capsule and track it readily all the way through to landing.

The preparation efforts conducted for Stardust cemented the sample return foundation that was poured during the Genesis efforts. Subsequent chapters will show how this foundation was required to construct range safety compliance analyses and strategies, defined the conditions under which the capsule was delivered to the atmosphere, was the backbone for developing operations timelines, and provided the landing ellipses for recovery operations planning.

# Chapter 3: Earth Targeting and Entry Safety Plan Volume 1: Safety Analysis

The concept of the Earth Targeting and Entry Safety Plan (ETESP) was architected during the Genesis Project as the method by which Earth sample return missions could describe the flight safety analyses and plans that would ensure compliance with applicable NASA and landing range safety requirements and policies. Ground operations safety considerations, those related to locating, handling, and transporting the recovered flight hardware and science samples, were included in the inaugural Genesis document. However, Stardust, prompted by observations from the Genesis mishap investigation pertaining to the dangers of multiple document content overlap, found these to better reside in separate recovery operations plans and procedures (see Chapters 10 and 11).

Together, the Stardust ETESP Volume 1 and Volume 2 (Chapter 4) demonstrated compliance with applicable requirements for protecting the safety of the public, workforce, and property associated with targeting, releasing, and delivering the sample return capsule (SRC) from deep space to the selected landing location on the Utah Test and Training Range (UTTR). Building from the baseline mission design and navigation plans described in Chapter 2, Volume 1 contained the safety assessment associated with flying the approach and entry trajectories, with appropriate accounting for low probability anomalies and failures, and provided the fundamental context upon which Volume 2, Decision Criteria, was built to ensure compliance throughout the flight operation. Approval of Volume 1 provided, in effect, overall approval to initiate the targeting and capsule release events.

## Safety Analysis Requirements and Preparation Architecture

The set of entry and range safety requirements that were applicable to the Stardust return were documented in NASA's Range Safety Program [ref 15] and UTTR's Range Commanders Council Standard [ref 16]. These documents established the allowable limits for risk to an individual (different for the general public or one involved in the recovery operation), risk to the population at large (or collective risk, also separated by general public and operations), and risk to property, including aircraft and waterborne vessels. In several instances these documents established different safety standards, and, in those cases, Stardust set forth to comply with the more stringent requirement. The requirements documentation also provided the sources of risk to be considered when demonstrating compliance: debris, far-field blast overpressure, and toxic material release, including radiological and biological.

The characteristics of the Stardust scenario and the availability of population and property data were such that one subset of the risk analysis quickly evolved as the primary task: human risk due to debris, i.e. direct contact between flight hardware and people with sufficient energy to cause damage. The energy threshold was established by the requirements documentation as 15 Joules, and was used in the identification of risk inducing debris. Assessment of the far-field blast overpressure, and toxic material release was completed fairly easily due to the relatively simple design of the Stardust hardware, the details of which will be provided later in this chapter. The biological hazard was avoided all together due to the Stardust Planetary Protection Category V designation for unrestricted Earth return.

The risk to property outside the landing range, as it turns out, is addressed specifically by NASA's range safety documentation, which states that complying with the human risk standards for the general public also provides appropriate protection for general property. There is a limit on probability of impacting property stated in the NASA documentation, however, discussions with NASA Headquarters revealed that it was intended to apply to high value assets related to the landing range and associated areas and such property was to be identified and managed directly with UTTR. To achieve compliance, five areas within UTTR were identified as landing keep-out

zones and the restriction of landing in those areas was incorporated into the ETESP Volume 2 decision criteria, effectively meeting the NASA standard.

On the other hand, bounding analyses were required and completed to show compliance with the risk standard for aircraft, and the contribution an aircraft related event would have toward the general risk posture for people. The details of those analyses will be described later in this chapter. No analysis was performed for waterborne vessels primarily because there was no reasonable database for that source of risk. In addition, it was felt its contribution to the general risk posture would have been much less than already conservatively examined in the other parts of the safety analysis.

***Human Risk Analysis Flow***

A very important component of the safety analysis was that it be conducted in a manner that ensured a confident result. To achieve this objective, at least two independent processes were used to validate every key step. The processes were implemented by different partnering organizations, each using their native tools and techniques, and each executed blindly until both results were available for review. Lead project engineers orchestrated and coordinated all activities, effectively policing the integrity of the process. A third party, independent of all the above, also monitored all steps in the process, performed analyses to spot check results, and aided in the reconciliation and convergence of results.

The safety analysis started with two parallel efforts. The first was the examination of the approach and entry trajectories, and possible spacecraft configurations and orientations with the goal of identifying scenarios that could lead to atmospheric entry, hardware breakup and burnup, and production of debris. This examination was conducted with the context of the biased navigation targeting strategy described in the Overview (Chapter 1), which progressively moved the trajectory's aim point from that of a flyby to that of Earth entry. One key result of this examination was identification of the event and the corresponding entry conditions for which the trajectory transitioned from skip out to atmospheric entry. The spacecraft divert maneuver was also examined during this activity, identifying the percentage of completion at which the outbound trajectory would no longer result in Earth entry. Part two of the initial effort was to conduct a complete inventory and characterization of the spacecraft and SRC components down to the box-level, including key items within each box. It would be these components that would be subjected to the breakup and burnup analyses associated with the different atmospheric entry scenarios. It was essential to achieve a correct and common understanding of the flight hardware to provide credibility to future result comparisons.

With the set of possible Earth entry conditions and an inventory of spacecraft components in hand, breakup and burnup analyses were conducted to produce preliminary reports containing a description of surviving components as a function of entry scenario. Recall, two independent organizations performed these analyses. Lead project engineers in conjunction with the third independent organization reviewed the methodologies that were applied, spot checked several instances of the analysis, and participated in the reconciliation of the results. The end product of this effort was a list of surviving debris that would be used in the population risk calculations.

For each item on the debris list, and each entry scenario, the next step in the safety analysis was to use the breakup and burnup history and propagate the item's trajectory through the atmosphere to obtain a landing location. With the addition of statistical navigation dispersions on the arrival of the spacecraft to the atmosphere and Monte-Carlo simulation of the atmospheric conditions during the item's descent, a series of landing ellipses were produced centered on particular locations on the ground. The center of a particular debris ellipse was designated the instantaneous impact point (IIP), and the inventory of debris ellipses laid out on the ground as a function of mission event was designated the IIP track. The length and width of the IIP track was essential in identifying the populated areas at risk from the Stardust entry operation. For efficiency, a single source was used for the majority of the debris ellipses produced during this

part of the ETESP effort. However, a limited spot check of the production process was conducted to achieve validation. The single set of debris ellipses also ensured that the subsequent safety analyses started from a consistent set of initial conditions.

Two independent groups compiled the collection of debris ellipses and, along with additional key assumptions for cross-section of interaction between a human and a debris item, ricochet factor, population sheltering (actually not used on Genesis or Stardust, more on this later), and probability of spacecraft failure, proceeded to calculate the corresponding risk to the general public and operations personnel. Both groups used the same population databases for inside and outside of UTTR. The population database for persons outside of UTTR was the main source for the calculation of risk to the general public. No operations personnel were assumed to be included in this database. The database for persons inside of UTTR was provided by UTTR safety officer, and specified which population was general public and which was participant in operations. Again, lead project engineers and the third party reviewed the methodologies that were applied, and spot-checked the analysis. The net result of these efforts were general public and operations personnel risk estimates for an individual person, i.e. the chance that a human has been hit by debris, and risk to the population at large, also designated collective risk, defined as the number of humans that are expected to be hit by debris. These different results were compared with the NASA and UTTR standards to ensure compliance.

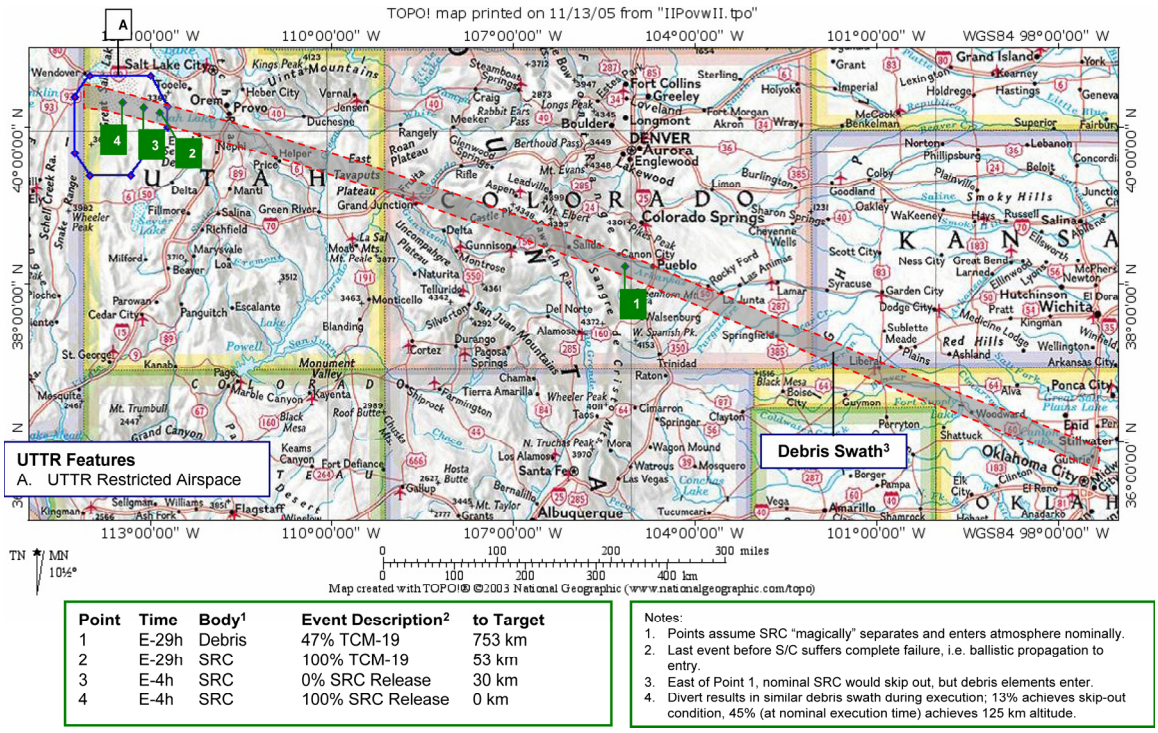
The end result of the ETESP safety analysis effort was a project document [ref S2] that was completed and signed off approximately one month prior to the Earth return event. Signature authority included project management staff, LMSS and JPL institution representatives, including an independent System Technical Warrant Holder, and a NASA headquarters representative. The bulk of the human risk analysis was completed in time for external review at the project's ETESP review performed approximately six months prior to Earth return. The safety analysis topic was additionally addressed as part of the project's system-level Risk, Implementation and Certification review. Delay in the publication of the document was driven by the need to address concerns identified through the review process regarding the validity of breakup and burnup tools in addition to the sensitivity of the analysis results to variations in fundamental assumptions.

## The Stardust Case Study

Five organizations contributed to the completion of the safety analysis on the Stardust. The Stardust Project System Engineer from JPL provided the leadership and overall coordination of the effort and authorship of the ETESP Volume 1 document. Also at JPL, the project's navigation team contributed by generating atmospheric entry conditions as a function of mission events and failure scenarios for both single and dispersed trajectories. A separate group of experts at JPL, not part of the Stardust Project, provided one of the reports on the anticipated breakup and burnup of hardware components. And finally, a third group at JPL conducted one of the sets of analyses that estimated the risk to the general public and operations personnel.

LMSS, the spacecraft contractor and operations partner, provided a group of experts, including lead systems engineers assigned to the project, who were the natural source for the inventory of spacecraft and capsule components. In addition, LMSS produced the second breakup and burnup report and supported validation of the debris ellipse generation process. Personnel from Langley Research Center's Space System division, part of Stardust to support entry, descent, and landing efforts, were the primary source of debris ellipses based on the breakup and burnup profiles and the navigation inputs. The fourth organization to contribute to the safety analysis was the Johnson Space Center's (JSC) Flight Dynamics division given their experience with Shuttle-based risk analyses. This experience was tapped to provide the second set of population risk estimates and additional validation of the debris ellipse generation process. JSC also provided the bounding analysis results for risk to aircraft. Finally, providing the "third party" perspective, the Aerospace Corporation fulfilled the broad, deep, and invaluable role of independent assessment, validation, and reconciliation of the key results produced by the primary analysts.

There were three propulsive events during Stardust's approach to Earth that dictated the size, shape and length of the Stardust IIP track: the final trajectory correction maneuver (designated TCM-19), propulsive activity between that final maneuver and capsule release due to unbalanced attitude maintenance, and the separation spring push-off of the capsule from the main spacecraft. Figure 3-1 shows how the incoming IIP track progressed from Oklahoma, up through Colorado, and to its final location within the UTTR. The outbound IIP track resulting from the divert maneuver (with and without an attached capsule) followed a similar enough track that its risk estimates were covered by latitude sensitivity analyses for the incoming track performed later in the development process.




| Point | Time | Body[1] | Event Description[2] | to Target |
|---|---|---|---|---|
| 1 | E-29h | Debris | 47% TCM-19 | 753 km |
| 2 | E-29h | SRC | 100% TCM-19 | 53 km |
| 3 | E-4h | SRC | 0% SRC Release | 30 km |
| 4 | E-4h | SRC | 100% SRC Release | 0 km |

Notes:
1. Points assume SRC "magically" separates and enters atmosphere nominally.
2. Last event before S/C suffers complete failure, i.e. ballistic propagation to entry.
3. East of Point 1, nominal SRC would skip out, but debris elements enter.
4. Divert results in similar debris swath during execution; 13% achieves skip-out condition, 45% (at nominal execution time) achieves 125 km altitude.

**Figure 3-1. Stardust Instantaneous Impact Points and Track**

The identification of atmospheric entry cases on which to perform breakup and burnup analyses was based on the trajectory and entry analyses that established the numbered landing locations (1-4) of the IIP track illustrated in Figure 3-1. Since the identification was a precursor to breakup and burnup analyses, these locations were the result of using an intact, stable SRC that could magically survive any entry condition. Four trajectory cases were selected for further analysis, bounded by the skip away condition (Point 1) and the planned entry trajectory (Point 4), with different combinations of spacecraft with and without the SRC and at different entry orientations.

Prior to proceeding with the breakup and burnup analyses, the ETESP teams met in a day-long workshop to ensure that all of the trajectory cases were properly identified and understood. In addition, the workshop served the purpose of reviewing the inventory of hardware components with special attention being given to items having high density, high heat capacity, and/or high melting point. Significant points of discussion were each item's material, wall thickness, mass, shape, size, and location within the spacecraft, specifically whether it was inboard, outboard and/or nested. Additional points of discussion were the failure criteria for all attachment interfaces and the predicted amount of propellant remaining in the single propellant tank.

All of the entry cases were examined by the JPL breakup and burnup team, with the LMSS team focusing on the most stressing and, as a result, most likely to yield debris. The LMSS team also performed studies to show and identify the point at which entering hardware would become

unstable and tumble, and, in the process, impart a corresponding tumble to the debris items released during the breakup process. In general, the LMSS approach to the breakup and burnup effort followed well-established NASA guidelines [ref 17]. The JPL team, however, after identifying which entry orientations and configurations were most stressing for each trajectory case, conducted its detailed analyses with a higher fidelity accounting of component location and protection from atmospheric heating, breakup time history, and resulting debris item shape, size, and corresponding coefficient of drag.

During the external review process, members of the review board found issue with the, perhaps perceived, limited amount of real-world data available to validate the tools used in the breakup and burnup analyses. These concerns were addressed by performing risk result sensitivity analyses through two independent approaches. The first was introduction of errors in the spacecraft component characteristics. The second was reduction of available aerodynamic heating combined with an increase in the failure criteria leading to breakup. Both of these would show the Stardust analyses to have significant amount of conservatism yielding margin that could offset the risk of analytical tools being wrong (see Safety Analysis Challenges for more details).

Several differences were encountered during the breakup and burnup reconciliation process: modeling of tungsten cubes as spheres versus tumbling cubes, survival or not of deck ballast, and the effect of G-loading on the capsule's heatshield (see Safety Analysis Challenges). These were solved, for the purposes of proceeding with the safety analysis, for the most part, by erring on the side of conservatism. For example, the list of surviving debris items that would be taken forward was constructed from the union of the lists generated by each of the LMSS and JPL teams. In addition, the entire debris list was assumed produced regardless of the entry condition or spacecraft configuration, despite the sensitivity that was found to exist. For Stardust, the surviving debris was comprised of the capsule heatshield, and eight tungsten cubes placed in the capsule's nose as ballast (see Appendix G). Similarly, capsule deck ballast was initially carried as a debris item into the risk analysis, but was later dropped from the operational procedures that supported ETESP Volume 2 when found to contribute an order of magnitude less risk than the heatshield and nose ballast.

In an effort to reduce the computational burden of the follow-on analysis, the initial collection of 26 debris ellipses resulting from the Langley's atmospheric propagation was winnowed down to 19 ellipses by grouping those cases that provided virtually indistinguishable debris ellipse sizes (within 2-3 kilometers, 1-2 miles). When reviewing the generation of these ellipses with external boards, the potential effect of aerodynamic lift, which was not being modeled, was brought into question. This concern was resolved by arguments that the spacecraft breakup was preceded by tumble, and as such there was no opportunity for lift to act on the departing components. Perhaps more convincing, however, was that, with an entry velocity of 12.8 kilometers per second (28,600 miles per hour), a very high magnitude lift would be required to change the shape of the resulting landing ellipses.

The policy of being conservative when possible was employed again during the final calculation of the risk estimates performed by JPL and JSC. Despite the entry occurring at 3 am local time, no risk discount was applied to account for sheltering of population. In addition, a generous 10% failure probability was used for the spacecraft, corresponding to the probability of there being a scenario that would lead to the production of debris. Only in one instance, support of the Yellow Divot (see Appendix C), was the failure probability decreased to 6%. The 10% value (and later 6%) was supported primarily by Stardust's 7-year flight history, and review of the capsule release mechanism reliability (Chapter 6). Vetted with external review boards, not only was the 10% generally accepted as conservative, but after consultation with safety personnel up through NASA headquarters, was deemed to not require support from a formal Probabilistic Risk Assessment. Subsequent examination of final results would show that as much as a 30% failure rate could be tolerated while still maintaining overall compliance with risk limits.

Armed with debris-human interaction areas calculated from the radius of a "standard" human and the surviving debris, and a ricochet factor of 2, given that the debris would fall nearly vertically to the ground, the JSC and JPL risk results found the collective risk to humans, i.e. the calculation of number of humans expected to be hit by debris, to be the driving range safety risk case. Both teams used the LandScan population database to represent the population outside of UTTR, and a database provided by the UTTR safety officer to represent population inside of UTTR. The NASA and UTTR human safety requirements were typically met by at least an order of magnitude, if not several. The collective risk estimate was closest to the UTTR standard, beating it only by a factor of 3.

During the integration of risk as a function of mission events, it was important, and proper, to separate those events that were separable by human intervention. In the Stardust scenario, the application of the ETESP decision criteria between the final trajectory correction and the capsule release event provided that separation. If there were to be a debris causing failure en route to the capsule separation, then the separation event would not occur. Likewise, if the separation event had been reached and approved without fault, then the risk prior to said event was effectively retired. And, while the core of the safety analysis focused on scenarios from the final trajectory correction maneuver through the divert maneuver, given examination of the baseline IIP track, the unbalanced nature of the Stardust attitude control together with the statistical nature of the navigation function created the need to verify that the risk standards would be met prior to this final correction maneuver.

To that end, compliance through the completion of the penultimate trajectory correction maneuver was met by purposely biasing the approach trajectory to avoid impact with Earth to greater than 4-sigma (or 1E-4). From the penultimate maneuver forward, the chance of Earth impact progressively grew in magnitude as a result of attitude maintenance activity, but the corresponding navigation deliveries to Earth, their interaction with the atmosphere (some trajectories entering, some skipping out), and the relatively paltry set of population centers under the potential, but very dispersed debris fields, when coupled with the low probability of a failure event actually occurring, were judged to not produce any significant risk. Additional mission scenarios were examined as part of the sensitivity effort to round out the risk robustness story, but are mentioned in this primer only as examples and are left as research for the reader: contingency trajectory correction maneuvers, maneuver overburn, separation with more than predicted spring performance, and extreme cross-track trajectory deviations (refer to the Stardust ETESP documentation, ref S2).

### *Ancillary Analyses*

As mentioned earlier this chapter, in order to provide comprehensive compliance with the UTTR and NASA requirements, additional assessments of risk to aircraft, far-field blast overpressure, and toxic material release were conducted as part of the ETESP effort.

The specific risk to aircraft was calculated only by the JSC component of the safety analysis team and was limited to airspace outside of UTTR. Access to the airspace within UTTR was strictly controlled and managed by Mission Control and was limited to recovery operation helicopters on the day of entry. As such, safety of the UTTR airspace was delegated to recovery operations preparations (Chapter 10) and was not included in the JSC analysis. For conservatism, the aircraft risk assessment used a uniform density profile ten times that of the Central California Valley to show compliance with the aircraft requirement with margin. In a similar manner, the contribution of an aircraft event to the collective general public risk was bounded by assuming that there would be no more than 100(!!) aircraft (or 10,000 people) under a debris ellipse at any given time.

Examination of the potential risks as a result of far-field blast overpressure, and toxic material release was relatively straightforward due to the simple design of the Stardust SRC. Breakup and burnup analyses described above showed that the entirety of the spacecraft bus, including

the propellant tanks and fuel, was consumed for all entry scenarios and as a result posed no risk. Within the capsule, the only potential sources of overpressure were the pressure vessels of the battery pack. However, these cells were hermetically sealed and equipped with a vent, thus posing no blast hazard. As far as toxic material release, the only source was ablation of the heatshield and backshell, which were predicted to ablate less than 2 kilograms (4.4 pounds) and 0.3 kilograms (0.66 pounds), respectively, easily dispersing and posing no risk to the ground. No part of the Stardust design contained radiological material.

## Safety Analysis Challenges

During the generation of the Stardust safety analysis, the project encountered several areas requiring additional attention to properly assess the risks involved in the Earth return operation. Spanning tool validation, fundamental differences in analysis assumptions, and a lack of knowledge over the behavior of first-flight hardware, these areas are captured here to illustrate the manner in which their risk was assessed, mitigated and/or, accepted (but effectively identified and communicated).

### *Concerns over Breakup and Burnup Tool Validation*

In the execution of the breakup and burnup analysis, LMSS used the same tool set that had been used for the design of many spacecraft aeroshells (Mars Pathfinder, Genesis, Stardust, Mars Exploration Rovers) and had been verified against other entry codes (Titan III Boost Ascent) and post-flight reconstructions (Viking and Pathfinder). Similarly, the JPL tool set was being used to support launch approval of New Horizons, Mars Science Laboratory, Jupiter Icy Moons Orbiter, and had naturally been used during ETESP analysis for Genesis. Nevertheless, when questioned, and subsequently researched, corroborating correlation to actual breakup and burnup events was found to be generally lean (Vehicle Atmospheric Survivability Test, Slender Hypervelocity Aerothermodynamic Research Probes, Reentry Atmospheric Flow Experiment), in particular for vehicles of the size of the SRC.

To address these concerns, the project performed two independent sets of analyses to establish the sensitivity of the risk analysis to errors in spacecraft component characteristics and/or errors in the fundamental physics of aerothermal heating. In the first analysis, hardware components were made 4 times more resistant to burning up. The corresponding breakup and burnup results showed that 4 to 9 more items would survive to the ground. However, said items were such that the stressing risk case (collective risk) only grew by a factor of 2 and remained below the required standard. The second analysis kept the original spacecraft component characteristics, but halved the amount of aerothermal heating imparted. In addition, the failure criteria for breakup were increased, delaying release of the debris. The maximum number of additional debris items produced via this experiment was 4, within the results of the first sensitivity analysis and, as a result, still below the required risk standard.

### *Sample Return Capsule Nose Ballast*

Eight, one inch, tungsten cubes were used in the design of the SRC to provide the required center of gravity location for stable atmospheric entry. The LMSS and JPL teams modeled these cubes differently resulting in significant disagreement on whether the cubes survived to the ground. Using NASA guidelines, LMSS modeled the tumbling cubes as spheres with a coefficient of drag of 0.9 (for relevant Mach numbers), and ablation during the burnup phase, but with no updates to mass, area or heating factors, and no radiative cooling. The end result was that the cubes did not survive to ground impact. JPL analysis, however, used tumbling cubes with a coefficient of drag of 1.4, applied both radiative cooling and ablation effects, and showed that the cubes did survive to ground impact. Literature searches and consultation with experts tipped the scales toward the JPL result. Aerospace's independent analysis also suggested the cubes were

more like to survive than not. Stardust adopted survival of the cubes based on the need to be conservative in the assessment of human safety issues.

The corollary to this decision, however, was that the assumed coefficient of drag would have a pretty significant effect on the landing location of the debris. For consistent application of Stardust's conservative policy, the project assumed the ballast debris could fall anywhere within the range predicted for a coefficient of drag ranging from 0.9 to 1.4. The analysis of the debris trajectories showed that the larger coefficient of drag resulted in a landing location farthest from the intact capsule IIP point. Subsequent safety analyses and operational procedures (in support of ETESP Volume 2) were constructed to take into account the possibility of landing anywhere within this larger ground distance.

***Sample Return Capsule Deck Ballast***

One, one inch, tungsten cube was used in the design of the SRC to provide spin stability during its flight to and through the Earth's atmosphere. In all but one JPL analysis case this deck ballast block was consumed. Nevertheless, the deck ballast was carried forward into the risk analysis phase. Only after inclusion showed a factor of 10 less contribution to individual risk and factor of 5 less contribution to collective risk was the object dropped from further consideration.

Wait a second now – a factor of 5 is still about 20% of the total, is it not? Ok, discarding the deck ballast from consideration was also supported by breakup and burnup results that showed the block arrived at the ground with less than the 15 Joules of kinetic energy required to be a source of risk to population or property.

***Sample Return Capsule Heatshield G-loading***

Both the JPL and LMSS breakup and burnup analyses showed that the SRC's heatshield, as might be one's intuition, was not consumed in any of the analyzed cases. However, the G-load limit for the heatshield remained unclear. As will be described in Chapters 5 and 6, the Stardust mission was the first flight of a phenolic impregnated carbon ablator (PICA) heatshield, and the capsule's entry speed, 12.8 kilometers per second (28,600 miles per hour), was the highest attempted. Pre-launch development used a design limit of 40-G and a testing limit of 50-G, but there was little knowledge of the performance of the heatshield beyond those limits.

Analyses conducted by the LMSS and JPL teams during the breakup and burnup effort showed possible maximum loading between 80-G and 100-G for the range of atmospheric entry angles under consideration. However, at the time of the Stardust flight, the knowledge of the PICA material was insufficient to do anything more than assume that, if the heatshield were to break up, the remaining pieces would be consumed since the aerodynamic properties intended to ensure survival have been defeated (single heatshield with specific size, shape and thickness).

## Special Topic: Validation of the Landing Target

During the initial review of the Stardust ETESP, the external review board was left with the impression, perhaps erroneously, given that the recovery operations review had yet to be conducted, that the project did not have an orderly process for selecting the location on UTTR to which the capsule would be targeted. The board was basing its conclusion on comparison to the very analytical landing site selection approach taken on Mars landed missions. Several board members also noted that human intuition was frequently at odds with the statistics of bi-variant Gaussian distributions (represented graphically by the predicted landing ellipse).

In response to the board's finding, the project, at the system-level Risk, Implementation and Certification review a couple of months later, not only described the recovery operations rationale for selection of the target (Chapter 10), but also presented a target validation analysis using the

construct of the ETESP safety analysis and decision criteria (Chapter 4). Compared to the Mars program approach, the recovery operations methodology was more visual in nature, and heavily based on the local knowledge of UTTR personnel, a component not readily available to Mars missions!

The ETESP validation process independently considered several contributors in the attempt to balance the risks involved in the selection process: best location for the incoming IIP track to maximize overall off-range safety compliance, probability of the final navigation estimate landing within an acceptable zone (for the purposes of approving the initiation of the separation event, and not to be confused with the probability of actually landing in said acceptable zone), and the probability of landing in a location that would be challenging for recovery operations (in mountains, in water, off land controlled by Dugway Proving Grounds – for all of these the SRC would still pass through the UTTR restricted airspace approved for Earth return). Weighting factors, naturally somewhat subjective, were assigned to each of these considerations prior to the analytical runs. Tools with heritage from the Mars site selection process were used to find an optimal landing location.

Quite surprisingly, the validation analysis showed that the location selected by the recovery operations team was within a kilometer of the location selected by ETESP considerations! This result was somewhat fortunate as use of the ETESP construct for the validation effort was somewhat controversial. The Stardust process was sufficient for an inaugural attempt at Earth return site selection and validation, but it was the opinion of many high ranking project personnel that the target selected by the recovery operations team with the local knowledge of UTTR personnel would not have been overridden by the analytical validation process. This is clearly an area for more growth in future sample return efforts.

## Summary

The creation of the ETESP construct as a response to the range safety requirements imposed by NASA and the landing range is, perhaps, one of the more important legacies both Genesis and Stardust have left to future sample return missions. The events following the Genesis mishap allowed for the refinement of the contents of the Stardust plan, appropriately left to deal, primarily, with protecting people and property during the execution of the final navigation and delivery of the sample to Earth.

The length of time available on Stardust for completing and reviewing the safety analysis effort allowed for a more in-depth and accurate product, and a more thorough understanding of compromising assumptions and unresolved (or irresolvable) risk. However, the Stardust return scenario and spacecraft characteristics serendipitously aided many aspects of range safety compliance and allowed the project to be very conservative with several key assumptions. These serendipitous characteristics also afforded the project the elbowroom required to perform sensitivity analyses in response to concerns over tools, methodologies and/or said assumptions.

A more detailed description of and the specific safety analysis results that were produced during the Stardust effort can be found in the ETESP volume 1 document [ref S2]. In addition, further Stardust specific lessons learned related to the safety analysis effort are documented in Appendix B: ETESP Volume 1 Lessons Learned and Appendix G: Vehicle Design.

# Chapter 4: Earth Targeting and Entry Safety Plan Volume 2: Decision Criteria

The development of the second volume of the Earth Targeting and Entry Safety Plan (ETESP) [ref S3], which focuses on operational entry criteria, benefited tremendously from the efforts of the Genesis mission. It was during Genesis that the fundamental architecture of the entry criteria was developed and, with the ability to start from an existing framework, the Stardust effort was able to identify and correct the weaknesses of the Genesis approach on its way toward developing the Stardust criteria.

The approach navigation strategy (Chapter 2), the results of the range safety analysis contained in ETESP volume 1 (Chapter 3) [ref S2], and the details of the sample return capsule (SRC) release sequence design (Chapter 7), developed concurrently, or as slight prerequisites, provided essential ingredients to the development of the project's decision tree and the decision criteria, in particular for range safety, described in this chapter.

## Overview

Compliance with the entry criteria, initially, accomplishes the goal of ensuring that the essential elements of flight operations associated with the safe delivery of the sample to the landing site have been successful, or have high probability of being successful during the separation events, and, subsequently, ensures that execution of the separation events do not violate the immutable range safety and landing site requirements. The criteria processes are one of the major linchpins for the final hours of flight operations for a sample return mission. As such, an operational decision tree or flow diagram was developed to establish a system-level guide for the terminal navigation, SRC release events, and information flow from flight operations to recovery operations.

Logically, the decision tree encompassed not only the elements required for successful implementation of the entry decision criteria, but also those operational pathways that were responsive to ensuring or protecting mission success (also see Chapter 7). Ideally, the framework established in the decision tree and criteria is then be used to develop the SRC release flight operations procedure. In recognition of these relationships, the ETESP decision criteria risk review was scheduled after the Mission Design and Navigation review (April), concurrent with the ETESP range safety review (early June), but before the SRC release sequence, and more importantly, the Flight operations reviews (late June).

On Stardust, the need to expand the existing, cursory, flight operations decision tree to a more complete, integrated, end-to-end version was not recognized until the Recovery (also late June) and Flight operations reviews. Development of the tree became one of the primary actions leading into the Risk, Certification and Implementation review (mid July), and subsequent Residual Risk reviews (through October). As a result, the full tree was developed after the initial plans and drafts of the operational procedures (flight and recovery) had been developed, and became more of a verification and validation tool and a method for communicating the project's general Earth return strategy. The reversal of this ideal development order was also due, in part, to the availability of Genesis Project materials that were similar enough to those required on Stardust to encourage a grab-and-modify approach.

The outcome of the ETESP decision criteria development process was a document that was approved by project management staff, LMSS and JPL institution representatives, including an independent System Technical Warrant Holder (representing an independent, technical authority as opposed to personnel in immediate supervisory roles), and a NASA headquarters representative. The approval process was architected so as to optimize the number of interactions required on the actual day of implementation. The ETESP strategy was initially laid

out and reviewed in the ETESP specific review, then progressively as part of the larger Flight operations context and ultimately the system-level context (refer back to Figure 1-8), providing confidence to the approvers, beyond their own personal review of the document, of sufficient rigor and independent assessment. The rationale for this approval structure was to enable the project team, those most familiar with the Stardust systems, to operate efficiently and quickly in the event of anomalies and untoward events as long as they remained within the pre-approved framework. Late in the criteria development, an appeal process for deviating from the pre-approved criteria was put into place (more on this later) to cover unknown scenarios, recognizing that every conceivable anomaly could not possibly be identified. However, the pre-appeal paths were fully recognized as inviolate in the absence of appeal, the opportunities for appeal were clearly designated, and the overall appeal process was constrained by time available.

The ETESP document was scheduled for completion by the time of the Risk, Certification and Implementation review in mid July. While the plans and detailed criteria for the document were fairly mature at that time, it was not completed until December due primarily to continuing fluctuations in the baseline mission and navigation strategies throughout the residual risk process, and late breaking discoveries during the test and training process. The decision tree was maintained informally (i.e. not tied to an official project document) throughout the residual risk and readiness review processes, and ultimately placed in the SRC release flight operations procedure. The operations procedure was only approved at the project level (i.e., no external approvals were required).

## Criteria Requirements and Architecture

NASA's Range Safety Program [ref 15], UTTR's Range Commanders Council Standard [ref 16], project documentation, and guidance from key JPL chief engineers encompassed the source of requirements for planning and implementing Earth return decision criteria. The NASA and UTTR requirements were related primarily to damage or danger to population and property, while project documentation related more to mission success. The guidance provided by the chief engineers provided the basis for landing site criteria that, if violated, would affect the recovery timeline, and could have institutional or agency implications as a result of missing the intended landing target.

The NASA and UTTR documents were effectively the same used in the development of the ETESP hazard analysis (Chapter 3), and, in fact, the bulk of project compliance was achieved through the Volume 1 effort (including far off-range population and property, aircraft, water-borne craft, toxic material release, far-field over blast, etc). Volume 1 contained an assessment of the risks to life and property associated with performing the final navigation targeting and the SRC Release activity, and provided the fundamental risk and hazard context upon which Volume 2 derived plans and criteria. While Volume 1 was the overall approval to initiate the targeting and release events, Volume 2 provided the mechanism to assess how the events were actually proceeding and allow (or disallow) continued execution. As such, the fundamental goals of the design of the criteria were to show compliance with the allowable risk to human casualties and property damage as specified by NASA and UTTR, to provide a high probability of the capsule landing inside a pre-defined acceptable region, and to return the science samples undamaged. A two-mechanism decision process was developed in response to these goals.

The first mechanism provided the opportunity to enable the SRC release command sequence upon confirmation that the navigation targeting had been successful, and that flight team personnel and required ground assets were sufficiently present, in place, and ready to monitor and respond to the execution of said separation sequence. Until this step was successfully accomplished, also in compliance with NASA directives, the spacecraft was defaulted to execute a divert maneuver, with SRC attached, forcing the flight system past Earth (and hopefully with the option for a backup opportunity, albeit years later, depending on the condition that lead to the criteria violation). This mechanism of the decision process was known as the Green Button;

compliance placed the mission in a "Go" condition for overriding the default divert and initiating the SRC release sequence. The Green criteria were fairly comprehensive to ensure that, indeed, all activity leading up to the initiation event had occurred as planned, but also because a wave off to the backup return opportunity was fairly benign from an SRC perspective: SRC battery depassivation (defined in Chapter 5) had not been attempted, and the electrical harness connecting the SRC to the spacecraft bus was still intact. Assessment of the status of flight personnel and ground assets was required to ensure the decision made with this first criteria mechanism could be implemented, and that the second mechanism would be fully supported.

The second mechanism of the decision process allowed for disabling the release command sequence in the event an anomalous event led to violation of the range safety or landing location criteria. Mission success, flight team, and ground asset criteria were removed from the abort considerations to minimize the probability of an abort given that the disable command could be sent at any time during the SRC release sequence, i.e. even after events had transpired that would place in jeopardy (battery depassivation) or eliminate (electrical harness severed) successful operation of the SRC during a backup attempt. Despite the risk to mission success, this second mechanism was essential in complying with the need to be completely safe with the sample return operation; personnel, property and landing location requirements took precedent over mission success. This mechanism came to be known as the Red Button (Stop!), and would interrupt the release sequence and jump to a divert maneuver, again with the SRC attached and with a higher consequence to the mission depending on where the interruption had occurred.

A third mechanism of the decision criteria architecture, developed for Genesis, was found to have no utility on Stardust. The goal of this third mechanism was to minimize the risks resulting from a contingency scenario where the spacecraft bus (the remaining carrier portion of the flight system) divert maneuver was compromised by a partial or weak SRC separation. Known as the Purple Button, its implementation would cancel the divert maneuver sequence prior to execution, thus allowing the entire flight system to enter the atmosphere, and break up and burn up along a trajectory that was fairly well known and in family with scenarios analyzed during the development of the range safety analysis. On Genesis, the electrical harness and a hinge connection between the spacecraft bus and the SRC, if not cleanly severed or separated, were such that the SRC would be left dangling from the spacecraft bus during the execution of the divert maneuver resulting in a highly chaotic dynamic system. In addition, the Genesis release and divert attitude geometries were such that if separation did occur, but provided a low separation velocity (due to weak separation springs), execution of the divert maneuver could lead to re-contact between the spacecraft bus and the free-flying SRC and, again, unknown dynamics. Under these scenarios, electing to implement the Purple Button was considered less risky than allowing divert execution to proceed.

On Stardust, this part of the criteria architecture was removed from the plan after determining that the Genesis risks were not present. Exploratory analyses found that a chaotic-divert debris ellipse was no worse from a range safety perspective than a no-divert debris ellipse. Furthermore, detailed examination of the flight system hardware revealed that in the event of a failure to sever the electrical harness there was no surplus length in the harness to allow the SRC to physically separate from the spacecraft bus. In addition, in the event of a failure in the separation mechanism, there was pre-loading in the mechanism arms to ensure sufficient spatial separation between the SRC and the bus prior to the initiation of the divert maneuver. Finally, the Stardust release and divert geometries were such that vehicle re-contact was a minimal concern. The Purple Button option was not required because the risks of chaotic dynamics during divert were avoided in the Stardust spacecraft design.

## Decision Tree

The objective of the decision tree was to provide a general description of the flow of events and information from start to end of the return phase, including low probability, but credible

contingency paths. Each event was noted with a time reference, and each branch or decision point was annotated with the responsible decision maker and a reference to an entry in a more detailed, supplemental, decision table. Figure 4-1 contains the first two pages of the Stardust decision tree as an example of the components of a decision tree (the full tree can be found in the SRC release flight operations procedure, ref F10). The location of the Green and Red Button evaluation events (two each) is also shown for context to the previous architecture discussion. Two evaluation events per mechanism were integral to the decision architecture to allow the opportunity for early detection of non-compliance and the chance to correct prior to the final evaluation. Also illustrated in the tree are the system-level interactions with anomaly procedures ("S/C anomaly"), on-board fault protection designs ("Safe Mode Entry"), mission success contingency commanding ("Swap C&DH sides"), and recovery team operations ("Provide Landing Loc.", "Provide.. to STRATCOM, RCS and LFACC"). Note that the tree consistently flows down for YES paths, and horizontally for NO paths. While obviously not required, this convention made obtaining an understanding of the tree more efficient and facilitated at-a-glance usage.

A companion decision table was created to ensure that the project team fully understood all the elements required to support implementation of the tree. This effort would eventually aid the validation of the proper information flow and development of staffing support plans and schedules. In addition, together, the two products were used to guide flight team test and training. Each entry in the decision table specified the decision being made, who was providing the information required to make the decision, what information was being provided, who the information was being provided to (the decision maker!), the possible outcomes of the decision, and, finally, the criteria (in as much detail as possible) that were to be used in making the decision. Figure 4-2 contains an excerpt of the Stardust decision table.

The baseline path through the decision tree and tables was relatively straightforward to design. As is frequently the case, the more interesting discussions revolved around the contingency paths, the number of them, and the level of detail to which the identified paths required specification. The answers to these questions typically came from examining the consequences of and available responses to a particular contingency scenario. For example, note there is quite a bit of detail regarding the contingency path resulting from navigation non-compliance at the first Green Button evaluation event (GB1, E-21h). The consequence of this branch was not only the obvious condition of not meeting the navigation criteria, but also the need to consider whether the non-compliance could or should be corrected. At this juncture, the final planned trajectory correction maneuver (TCM) had been completed and the final opportunity for a contingency TCM was only hours away. Unfortunately, due to TCM execution characteristics, the contingency TCM (at E-12h) did not necessarily result in better performance or chance of success than the baseline TCM (E-29h) (refer back to Chapter 2).

Whether the TCM was to be executed would depend on the source of the anomaly, the extent of the non-compliance, and the characteristics of the TCM. It was system-level complexity of this nature that warranted inclusion of this contingency scenario in the decision tree and table. For other contingency scenarios, the response was not as complicated, but the consequences were as severe. For example, an unsuccessful SRC battery depassivation (E-4:32) would very likely lead to a failure to energize the SRC avionics, failure to deploy parachutes, and a hard landing. The detection of the failure was captured in power telemetry; the response was to swap to secondary hardware. There was minimal complexity in this process, but the consequence warranted inclusion in the decision tree.

## Decision Makers

As was mentioned in the introduction to this chapter, it was considered essential on Stardust (and Genesis, for that matter) to leave the actual implementation and execution of the ETESP decision criteria in the hands of the project team. Empowering those most familiar with Stardust plans and systems provided the capability to quickly respond to anomalous events and decide on a course

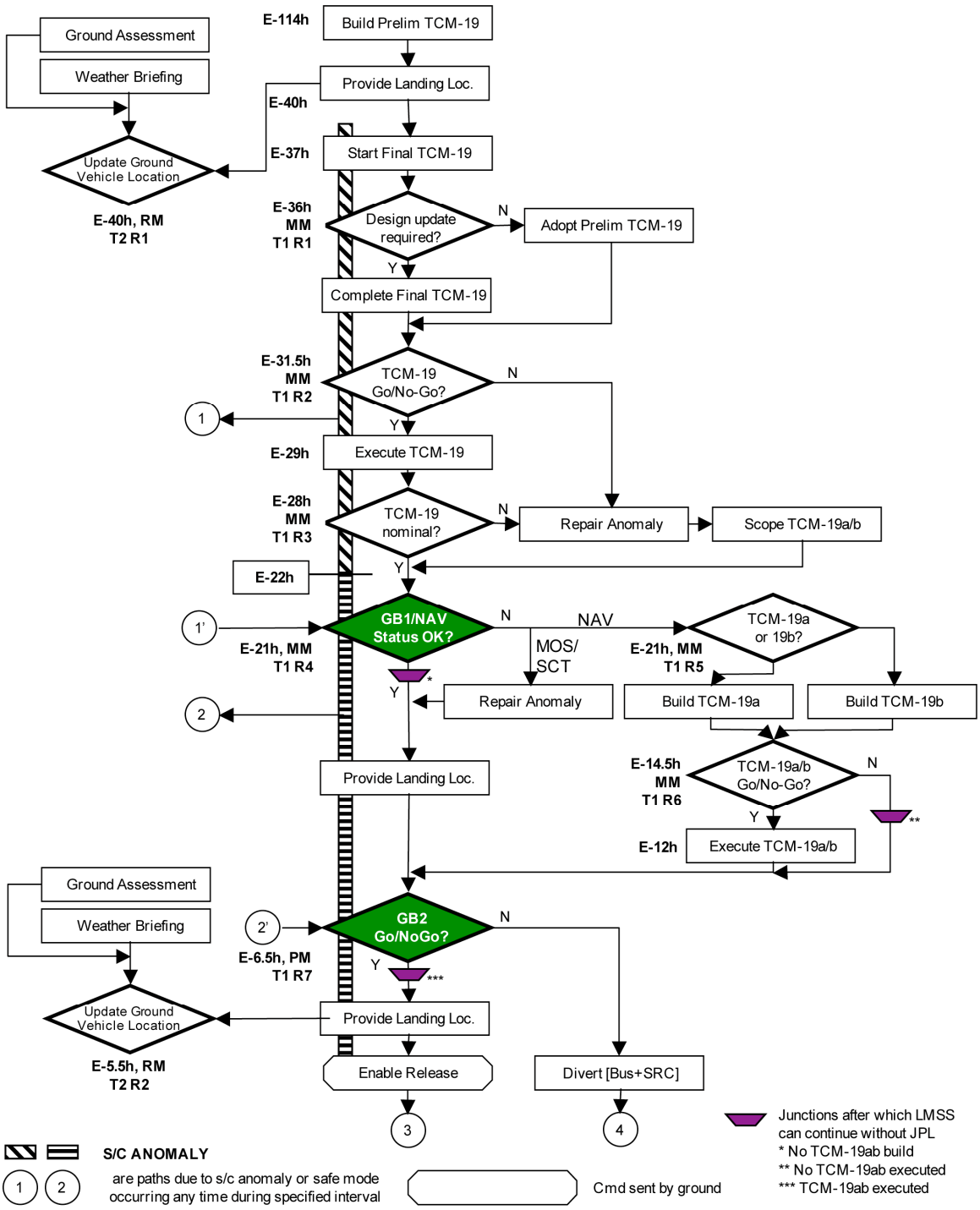



**Figure 4-1a (1 of 2). Entry Decision Tree (Partial Flight Operations)**

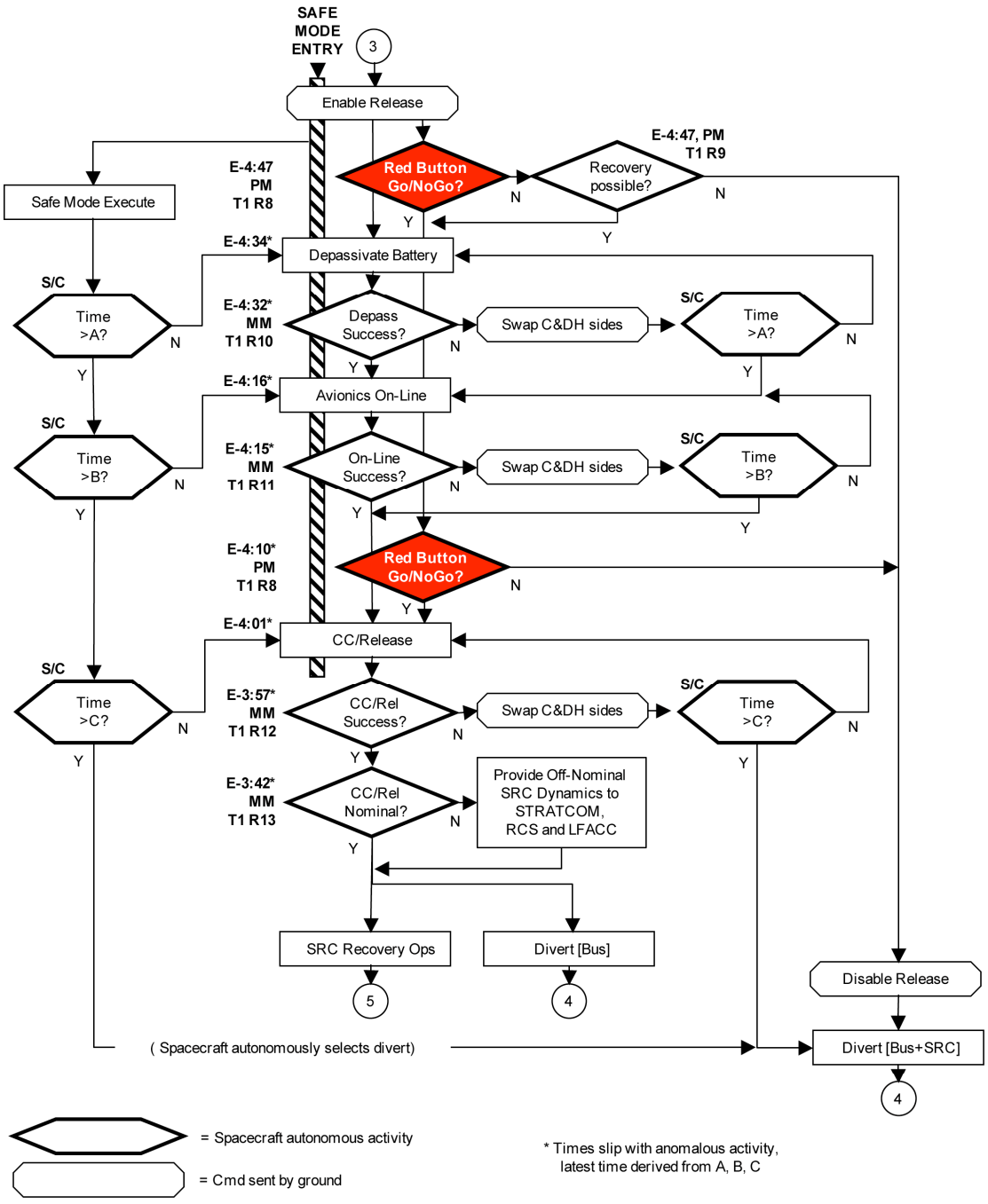



**Figure 4-1b (2 of 2). Entry Decision Tree (Partial Flight Operations)**

| Entry | Decision | Data Providers | Inputs | Decision Maker | Outcome |
|---|---|---|---|---|---|
| 1 | TCM-19 Preliminary or Final | NAV Team Chief<br>Spacecraft Team Chief | NAV Assessment<br>SCT Assessment | Mission Manager | Select preliminary TCM-19 design or complete final design and prepare for uplink |
| Criteria | | | | | |
| a | Has the TCM magnitude changed by more than 5 mm/s? If yes, build final, if no adopt preliminary. | | | | |
| b | Maneuver magnitude greater than 0.5 m/s ? If greater than 0.25 m/s, discuss/discretion, if less than initiate 19a/b option. | | | | |

| Entry | Decision | Data Providers | Inputs | Decision Maker | Outcome |
|---|---|---|---|---|---|
| 2 | TCM-19 Go/NoGo | Systems Lead<br>NAV Team Chief<br>Spacecraft Team Chief | Sequence Products<br>Uplink Summary<br>Spacecraft Health | Mission Manager | TCM-19 Sequence Approved or Not for Uplink |
| Criteria | | | | | |
| a | Command products approved per uplink summary? | | | | |
| b | NAV verified burn parameters? | | | | |
| c | Spacecraft capable of performing TCM? | | | | |

| Entry | Decision | Data Providers | Inputs | Decision Maker | Outcome |
|---|---|---|---|---|---|
| 3 | TCM-19 execution nominal? | Spacecraft Team Chief<br>NAV Team Chief | S/C Telemetry<br>NAV Tracking Data | Mission Manager | Identification of Anomaly Repair Strategy<br>Initiate TCM-19a/b option<br>Or nominal, no additional action required |
| Criteria | | | | | |
| a | Maneuver execution less than 0.5-sigma from prediction? [<10 km from target] | | | | |
| b | No safe mode entry? | | | | |
| c | No anomalous subsystem performance? | | | | |

| Entry | Decision | Data Providers | Inputs | Decision Maker | Outcome |
|---|---|---|---|---|---|
| 4 | SRC Release Enable preliminary evaluation, conditions met? | Spacecraft Team Chief<br>Navigation Team Chief<br>MOS Team Chief | S/C Telemetry<br>NAV Reconstruction and EDL propagation<br>GDS Status | Mission Manager (concurrence: MOA, ETESP Mgr) | Identification of Violation<br>Initiate Corrective Action<br>Build TCM-19x<br>Or nominal, no additional action required |
| Criteria | | | | | |
| a | SCT SRC Release Enable Criteria Table | | | | |
| b | MOS SRC Release Enable Criteria Table | | | | |
| c | NAV SRC Release Enable Criteria Table, with and without TCM-19b if applicable (off-nominal delivery known prior to meeting) | | | | |
| d | Is landing location less than 15 km from the target? If Yes no need for TCM, else build TCM to correct back to target | | | | |

| Entry | Decision | Data Providers | Inputs | Decision Maker | Outcome |
|---|---|---|---|---|---|
| 5 | Build TCM-19a or TCM-19b? | Navigation Team Chief | NAV Reconstruction and EDL propagation | Mission Manager | Use TCM-19a build or TCM-19b |
| Criteria | See TCM Build Map | | | | |

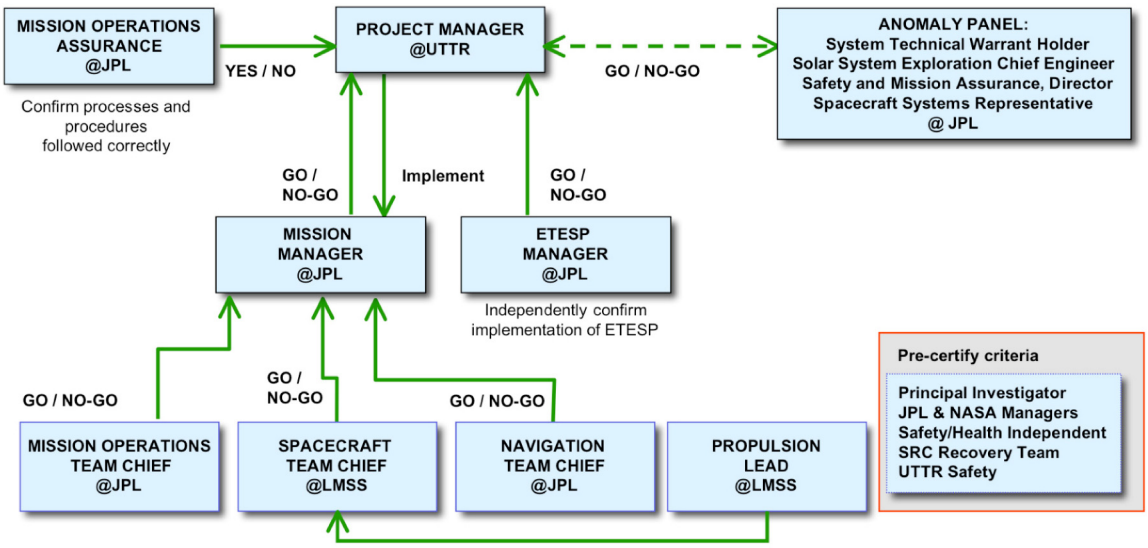
| Entry | Decision | Data Providers | Inputs | Decision Maker | Outcome |
|---|---|---|---|---|---|
| 6 | TCM-19a/b Go/NoGo | Systems Lead<br>NAV Team Chief<br>Spacecraft Team Chief | Sequence Products<br>Uplink Summary<br>NAV Assessment<br>Spacecraft Health | Mission Manager | TCM-19a/b Sequence Approved or Not for Uplink |
| TCM GO/NO GO | | | | | |
| a | Does TCM-19b option increase the probability of a successful SRC Release enable meeting? [Reference Trade Spreadsheet] | | | | |
| b | Does the OD solution have a trend in it? Is the trend credible, or a statistical artefact? | | | | |
| c | Is the spacecraft able to perform a TCM? | | | | |
| d | Have previous recent TCMs been anomalous in performance? | | | | |
| e | Is the required TCM size below 0.5 m/s? Below 0.25 m/s? | | | | |
| f | Is the spacecraft using secondary hardware? | | | | |
| g | What is the general state of the health of the spacecraft? | | | | |
| h | What is the space/solar environment? Has it been the cause of any spacecraft anomalies? What is the future prediction? | | | | |
| COMMAND CONFERENCE | | | | | |
| a | Command products approved per uplink summary | | | | |
| b | NAV verified burn parameters | | | | |

| Entry | Decision | Data Providers | Inputs | Decision Maker | Outcome |
|---|---|---|---|---|---|
| 7 | SRC Release Enable FINAL evaluation, conditions met? | Spacecraft Team Chief<br>Navigation Team Chief<br>MOS Team Chief | S/C Telemetry<br>NAV Reconstruction and EDL propagation<br>GDS Status | Project Manager (concurrence: MOA, ETESP Mgr) | Enable SRC Release or allow Divert |
| Criteria | | | | | |
| a | SCT SRC Release Enable Criteria Table | | | | |
| b | NAV SRC Release Enable Criteria Table | | | | |
| c | MOS SRC Release Enable Criteria Table | | | | |

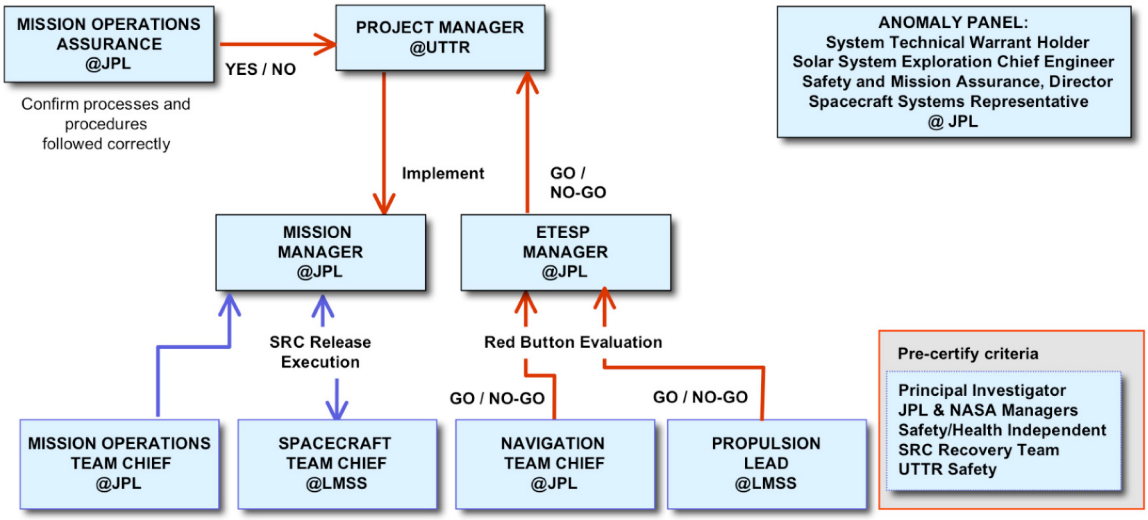
**Figure 4-2. Entry Decision Table (Partial Flight Operations)**

of action. Relevant non-project personnel, in particular document signatories, were provided the opportunity to review, comment and pre-approve the construct within which the criteria were to be implemented and the detailed criteria, observables, triggers, rationale, and outcome sensitivities to different stimuli (the latter primarily through test and training activities).

Figure 4-3 shows how implementation of the SRC release enable (Green) and disable (Red) functions stayed within the project, and who outside the project was granted the specific opportunity for review and approval (or "pre-certification"). Implementing a lesson learned from Genesis (workload and independent reporting), the position of an ETESP manager was created on Stardust to allow the Mission Manager, in particular during the SRC release sequence and disable process execution, to focus their attention on mission success while the ETESP manager focused on the disable criteria. The function of the ETESP manager was best compared with a launch range safety officer; a function the bulk of the community was familiar with for independent safety during launch operations. Although there was a UTTR range safety officer that was independent from the flight team, for the sample return scenario, and for Stardust, complete project independence of this function would have been too costly (in time and effort) and inefficient. The carrier vehicle was the Stardust spacecraft itself and implementation of the criteria, and interpretation of the input data benefited from (and perhaps required) intimate knowledge of Stardust systems.




**(a). SRC Release Enable**




**(b). SRC Release Disable**

**Figure 4-3. Decision Criteria Approvers and Implementers**

Two items in Figure 4-3 may be the source of curiosity: the lack of involvement of the SRC recovery team, and the presence of an anomaly panel. The first is the result of there being no recovery team criteria (weather, landing site conditions, equipment, personnel, etc) that would affect the decision of whether to allow the capsule to be released. There will be more details on the rationale for that construct in the next section. The anomaly panel, however, was the direct result of finding an error in the decision criteria during test and training and having no avenue to appeal the outcome though it was analyzed to be benign. An anomaly appeal process was lacking during the Genesis Project as well, but an informal one was implemented during the last few days of the mission when a benign error was also found in that decision criteria.

The lack of a documented appeal process came to a head during an SRC release enable (green) meeting of one of the operational readiness tests (ORT) conducted during the return preparations. A thruster firing frequency criterion, which had been established due to its association with unplanned velocity changes, was shown to be in violation. However, while the criteria trigger had been set to catch anomalous behavior, the scenario supposed a step function in the frequency with no further degradation and at a level that, when applied to the navigation targeting, did not move the landing location outside of the desired region. The flight team very quickly became divided between those that remembered Genesis and sought to appeal the criteria given the evidence of still landing inside the desired region, and those who stated there was no process or allowance for the appeal and that the project must decide against enabling the SRC Release event. At this point the ORT basically stalled, the issue was tabled, and the test conductor made a real-time intervention to allow the ORT to continue.

The ensuing post-test discussion resulted in the implementation of the anomaly panel. Its function was applied only to the SRC release enable process as it was then that there would be sufficient time to craft, document, and present the arguments that the panel would need to hear to override the documented, pre-approved, criteria. Needless to say, the thruster frequency criterion was also examined, but that examination evoked a different dilemma: quantitative versus qualitative criteria, a challenge that will be discussed further in a few pages.

## Detailed Criteria Development Process

The detailed criteria development process started with establishing high-level guiding synopses. These synopses captured in clear, understandable language, the intent of the SRC release enable and disable mechanisms and reflected the driving requirements that flowed into the detailed criteria development. They summarized the purpose of each decision mechanism and what motivated their existence. For example, the SRC Release enable purpose was stated as “Spacecraft will divert to backup orbit with fully functional SRC if command is not sent”. The motivations for the enable, for Stardust, have in fact already been stated earlier in this chapter: recovery with negligible probability of population and asset damage, recovery with high probability of landing inside the acceptable region, high confidence in the spacecraft’s ability to perform SRC release events, high confidence in the ground’s ability to monitor and respond to spacecraft activity, and return the science samples undamaged.

The next step in the development process was to identify those groups or teams within the project that would be able to contribute to showing compliance with the motivation (or requirements) statements. One of the key components of this process was to find a balance that provided rigorous, somewhat unique, but also collaborative contributions to the evaluation process. Too many contributors and the process would become unmanageable, but too few and the process would not be sufficiently comprehensive. On Stardust, the navigation team was ideally situated to provide the inputs for all range safety, and landing location criteria. They also ended up providing the input for the sole criteria on science sample safety. The spacecraft team was best suited to provide the inputs for the health, safety and status of the spacecraft itself. The mission operations team was best suited to providing the inputs on the ground hardware, software, and personnel.

Note the absence of recovery considerations in both the criteria motivation and the team participation. This characteristic was by design and was a reflection of the desire to drive to an absolute minimum the number of items that could result in an aborted attempt to release the SRC. The project's mitigation to any landing site contingency was the development of detailed contingency plans (Chapter 10), a lesson learned from the Genesis mishap experience. These contingencies included, but were not limited to bad weather, landing in a bad location (mountains, water hazard, near unexploded ordinance [UTTR is an active bombing range], etc), equipment problems, and personnel problems. Each of these contingency scenarios was considered low probability, but credible and with severe consequences to recovery of the science samples in an undamaged state. However, they did not pertain to range safety, achieving the landing location, the spacecraft's ability to accomplish the SRC release, or the SRC's ability to perform the entry, descent, and landing activities. The risk of having to implement the back up opportunity (i.e. flying the vehicle for 4 more years, which amounted to a 57% lengthening of the mission) was deemed higher than having to implement any of these recovery operations contingencies.

Continued development of the decision criteria was comprised of determining a series of specific statements that would answer the different components of the driving requirements. Identification of observables and supporting rationale completed the criteria description and closed the loop with the motivation and driving requirements. Initially, a table of contents of the observables was developed, but as scenario analysis, sensitivity studies, and test and training progressed, the specific values and trigger levels could be filled in and verified. An illustration of one component of this process was provided with the previous description of the thruster firing frequency criterion. Another example of this validation process also presented itself during test and training and resulted in the sole SRC release enable criteria for science sample safety: entry flight path angle (see Criteria Challenges).

## Tools and Training

The final step in the decision criteria task was to ensure the proper ground hardware and software were available and certified for use in the specific criteria evaluation application, and that personnel were trained and certified in using said hardware and software.

For the most part, the hardware and software used to complete the evaluation of the criteria were used in day-to-day operations and did not require additional certification – spacecraft health and safety, ground equipment status, navigation orbit determination and maneuver design, etc. Others were used specifically for the return phase, but had been used on other missions in similar applications: Genesis Earth return, Mars Exploration Rover landing site hazard analysis (though not as simple as replacing rocks with people). One software tool was considered for new development during the Stardust return phase. Its function would have supported, and, in fact, automated the navigation team's monitoring of radiometric data and corresponding velocity change profile for detection of unplanned events as was required for the SRC release disable (red) process. The decision was made to not develop this tool and instead implement a manual process (with Genesis heritage) due to schedule and financial constraints. The project's decision was reviewed and approved by both external review boards and institutional representatives, and validated during test and training.

Regardless of the heritage, one of the least desirable anomalies was for a mistake to be made during the evaluation process by a tool that was believed to be operating correctly, but when presented with a unique Stardust scenario, would fail to either provide the correct answer or would not be capable of providing the answer in the required time. The tools needed to do both to support the decision criteria timelines. To ensure the tool suite was certified to support return operations, a compliance matrix was constructed with the following elements: Name, Function, Software Certification Category, Cognizant Engineer or Institutional Group, Failure Risk Assessment, Participation in Formal Project Testing, Participation in Formal Unit or Acceptance Testing.

Flight team training was accomplished with a comprehensive test and training program (Chapter 7) comprised of procedure briefings (2), criteria scenario discussions (2), thread or data flow testing (multiple), procedure rehearsals (2), flight team operational readiness tests (1), and, finally, end-to-end, integrated, system-level operational readiness tests (1, with the opportunity for a make up for any failed components). The lessons learned during the program, and value to validation of the entry criteria, are sprinkled throughout this chapter.

## Criteria Challenges

The construct and detailed content of the Stardust ETESP decision criteria evolved throughout the development process in an effort to ensure that the correct and proper set of elements were guiding the decision to allow (or not) the SRC release event to occur. The evolutionary process was the result of continual examination of scenarios, discussion of what was proper and responsible, test and training, and, ultimately, achieving the correct answer to the question: "Do we really want to wave off the return and go to the backup orbit for that?"

### *Qualitative versus Quantitative Criteria*

The thruster firing frequency criteria incident that presented itself during test and training left the project to struggle with the fundamental architecture of the specific criteria statements. The spacecraft health and readiness criteria triggers were originally selected to trap atypical behavior because it was deemed the conservative approach to take, i.e. if the spacecraft is not performing as expected or predicted then why should the project feel safe proceeding with the SRC release operations? However, the firing frequency incident posed a scenario where the spacecraft's behavior could be atypical and yet not lead to violation of the higher level, stricter driving requirements captured in the navigation criteria.

The project's approach to solving this dilemma was to replace the existing specific, quantitative criteria for spacecraft and mission operations with more general, functional, qualitative criteria backed up with quantitative "indicators". The goal was to allow the evaluator of the criteria to interpret the indicators, and apply their experience in providing a compliance assessment to the qualitative criteria. Rigor in the process was maintained by requiring the criteria evaluator to provide proper rationale in the event an indicator was in violation, but the qualitative criteria was still deemed met. For example, the problematic firing frequency criterion was converted from: "RCS Thruster On Time Rate < 2 sec per sec" to "Is the thruster performance predictable?" with the former specific criterion downgraded to an indicator. This construct, in the scenario encountered during the test and training, would have allowed the qualitative criteria to be shown as met as long as the violation of the frequency indicator carried the appropriate explanation as to why it was still considered predictable, along with a corresponding statement about residual risks and implications to the overall mission.

When the changes to the project's decision architecture were subject to external review, not surprisingly, two camps formed within the review board! The first felt that, in conjunction with the addition of the anomaly panel, the conversion from quantitative to qualitative criteria was unnecessary and perhaps dangerous. That, the project was softening up the criteria structure and there were now too many avenues for interpretation and human intervention. They advocated that the entry criteria should be crisp, clear and concrete, much like launch criteria, and that the project should be able to select quantitative triggers and stick to them. If violated, the avenue to pursue was the recently added anomaly panel. A second camp, in effect, agreed with the project's new architecture and additionally suggested that it created an environment where any given analyst would feel more comfortable reporting an anomalous reading or anomalous behavior as it would not lead immediately to a criteria violation and aborting of the SRC release event. The review board findings concurred with project's new plan, but made sure to acknowledge the dissenting opinions.

### *The Anomaly Panel*

The late addition of the anomaly panel was, as has been described, an attempt to ensure that if a criterion was found to be in violation, the project had the opportunity to explore the possibility of continuing the SRC release operations outside the bounds of the pre-certified process. To not be slave to the "ink on the page", in the event the situation that was being faced was indeed benign, but had simply not been anticipated. Once added, the anomaly panel was carefully architected to prevent the creation of a loophole for the project to violate criteria and be allowed to proceed. As a start, not all of the entry criteria were available for appeal. Human safety and property damage requirements set by NASA and UTTR were top priority and would not be open for debate.

For other key criteria, landing within a pre-approved region, and delivery of the SRC within the certified range of entry flight path angles, the anomaly panel, based on information from the project, defined not-to-exceed limits. These limits were beyond the values that triggered a project violation, however, allowed for some leeway in the event of a contingency scenario, while establishing a level of excursion beyond which the violation would not be waived regardless of the scenario. In addition, the anomaly panel was comprised of four senior institution engineers (directorate heads, chief engineers) from JPL (3) and LMSS (1), independent of the project, but well versed in Stardust due to their participation on risk and readiness review boards, and able to understand the technical detail, the project perspective, and represent the institution and agency in their deliberations. A complete, unanimous vote was required to approve the project's appeal.

### *Landing within a Pre-Defined Region*

The most debated criterion within the entry criteria suite was the one that established the need to land the SRC within a pre-defined boundary of the recovery operations area. For Stardust (and Genesis), this meant landing within the boundaries of the restricted airspace of UTTR. One of the key elements of this criterion, however, was to what probability? To a 99% probability, to 95%, lower? Consider the discussion in light of a baseline navigation capability that predicted landing inside of this region to just about 6-sigma (99.99999%). As of the publication of this document, there is no guiding document or requirement that establishes the need for the criterion, much less the level to which it should be met. If such was true, why have the criterion at all?

The answer, at least for Genesis, which set the precedent, and Stardust, which followed suit, was that it was the proper and responsible thing to do, in spite of the possible implications to mission success. The projects felt duty bound to ensure landing within the confines of the UTTR landing site, where they were approved to conduct operations, and where the infrastructure existed to perform the recovery activity. This posture was supported by other well thought out rationale: eases recovery logistics (keeps the public away from the capsule); avoids the unknown consequences (public perception, future sample return) of missing, by so much, the intended target; if missing by so much, something assuredly has gone wrong with the spacecraft. However, these were challenged by equally valid arguments regarding the risk of having to fly the spacecraft to the backup opportunity (more so if an anomaly has already occurred), in conjunction with those that noted the sparse population near the western boundary of UTTR and the correspondingly very low probability of violating the NASA and UTTR range safety population and property requirements.

As for selecting of the probability with which the landing location criterion was to be met, the values for Stardust were based a consensus engineering judgment involving document signatories, institution chief engineers, and project personnel, with corresponding vetting up the chain-of-command with NASA headquarters and the NASA safety office.

### *Criteria Assumptions and Validation*

The test and training program showed its value once again during an ORT that revealed an inconsistency between the requirement to land within the approved area on UTTR and the

certified limits of the SRC's entry flight path angle (a key parameter used to describe the tolerable aerothermal environment during entry). During the construction of the navigation criteria, it had been assumed that the certified entry flight path angle was broad enough, or close enough, to encompass all the trajectories that would land within the approved area on UTTR. And it fact, while it was close, the scenario presented during the ORT placed the landing ellipse prediction still within the required landing limits, but with a uncomfortably large fraction of the entry flight path angles associated with those trajectories outside the certified angle limits.

Further investigation into the discrepancy revealed that the criteria builders, in consultation with the SRC thermal protection system designers, had answered the question of whether they would want to abort the return, if faced with entry flight path angles slightly beyond those certified, with a resounding "NO". However, having done that, they had not only invalidated the extensive re-certification effort for entry flight path angle (see Chapter 6), but also short-circuited the appeal process and removed one of the mechanisms via which risks were communicated and accepted by the chain-of-command both in the design and implementation of the return operation.

The result of this interaction was a very late addition of an entry flight path angle criterion to the existing suite of navigation criteria. Concerning primarily mission success, this criterion was subject to appeal to the anomaly panel, which also went through the exercise of defining a not-to-exceed limit.

## Summary

Being the second incarnation of the ETESP concept, the Stardust decision criteria effort was a significant improvement over the Genesis effort in terms of in-depth understanding of the driving requirements and the sensitivity of the resulting criteria to various stimuli. However, as one might gather from some of the challenges described herein, there remains room for improvement.

Perhaps most relevant for future ETESP efforts is further discussion on the issue of qualitative versus quantitative criteria in the context (or not) of an anomaly panel. This change was identified late in the development process and alternate solutions or problems might have been found given additional time for testing and training, and scenario discussion. This and the other challenges faced during the Stardust decision criteria effort showed the value and role test and training can play in the development effort and the need for continuous and rigorous system engineering.

The specific, final decision criteria that resulted from this effort can be found in the ETESP Volume 2 document [ref S3] and the SRC release operations procedure [ref F10]. In addition, further Stardust specific concerns and issues are documented in Appendix C.

# Chapter 5: Sample Return Capsule System Review

The entry, descent, and landing (EDL) elements of the Stardust sample return capsule (SRC) were dormant for the bulk of the Stardust mission, designed to be initialized a few hours prior to Earth return and triggered to operate upon capsule interaction with the Earth's atmosphere. As such, the EDL event was effectively one rather important first time event for Stardust. While risk assessments had been performed during pre-launch development, they were reassessed in the year before Earth return due to the revised review requirements described in Chapter 1 and the Genesis Mishap Investigation Board (MIB) recommendations for Stardust. This chapter addresses the SRC 'as-built' system risk assessment, including those elements from the spacecraft associated with SRC release, with the exception of the aerothermal and parachute risk assessments. Those elements are discussed in Chapter 6, Entry, Descent, and Landing System Review.

## Sample Return Capsule Background

The Stardust SRC and some of its features are shown back in Figure 1-2, in the lower right. The design requirements for the SRC were to house the aerogel in a way that it could be deployed for sample collection, then stowed away for atmospheric entry at a velocity that was higher than any previous man made object. As a result, the SRC needed a thermal protection system (TPS) more capable and lighter than any previous capsule, and it had to be stable until slowed sufficiently that a parachute could be used to provide stability at subsonic speeds, where blunt capsules were known to be unstable.

To stay within Discovery Program cost constraints, the SRC was designed to be a "passive" capsule with no active trajectory control and simple functions. Hypersonic stability was achieved with a center of gravity (c.g.) that was ahead of the hypersonic and supersonic centers of pressure; it was necessary to add mass in the nose of the SRC to achieve the required c.g. location. Hypersonic stability was aided by starting free flight with a spin rate of sufficient magnitude to provide gyroscopic stiffness relative to atmospheric disturbance torques, but not so stiff that the capsule would not be able to remain aligned with the flight velocity vector. To impart this spin prior to free flight, a three axis controlled spacecraft such as Stardust could have been spun up prior to separation, but the lack of a balanced thruster system would have introduced errors and challenges to achieving accurate capsule release and corresponding navigation targeting. The Stardust solution was a separation/spin mechanism that simultaneously provided the required velocity and spin rate during separation from the spacecraft.

The battery that was used on the SRC, active only during entry, was selected due to its long-term storage capability. It was an assembly of primary lithium sulfur dioxide cells used extensively in military applications. The battery formed a high resistance passivation layer early in storage, which required depassivation with high current prior to use for entry (more on depassivation later in this chapter and see Chapter 7 for details on the SRC release critical command sequence). The SRC avionics unit (AU) used acceleration switches (also referred to as G-switches) designed to close when deceleration forces rose above 3 G's, and open when the deceleration dropped below 3 G's. This activity then initiated timing circuits, with a simple resistor-capacitor low pass filter to take out switch chatter, for pyrotechnic release of the drogue and main parachutes. The drogue parachute was timed to deploy at about Mach 1.4 to stabilize the capsule, while the main parachute was timed for about 10,000 feet (3048 meters) for the slow final descent. A final pyrotechnic cutting of the main parachute lines was performed to prevent the wind from dragging the SRC. This event was enabled by timer, but activated by a second acceleration switch upon landing.

The AU also contained an ultrahigh frequency (UHF) transmitter with an antenna up a main chute riser to aid in tracking during final descent and in locating the SRC after landing. Block redundant

batteries, and timing and firing circuits were incorporated to assure robust EDL functional performance.

## Sample Return Capsule System Risk Assessment Process

The general plan for assessing the risks in the SRC system was to gather design, analysis, test, and verification and validation documentation, conduct a series of table-top-reviews with area experts, and perform additional analyses and tests where needed to fill in the documentation gaps. A team of Jet Propulsion Laboratory (JPL) electronics engineers and a system engineer, along with the Lockheed Martin Space Systems (LMSS) system engineering lead, performed an in-depth review of all facets of the SRC system's ability to perform all entry functions. They were supported by LMSS project personnel who complemented the detailed information contained in existing documentation and performed select analyses. An important thrust of the risk assessment effort was the review of component-level testing, the assembly and test flow at the SRC level, and the integrated system test flow with particular emphasis on the test-like-you-fly exceptions.

The 'as-built' team participated in an initial SRC-specific risk review, the project-level Risk, Implementation and Certification review, and a Residual Risk review, with review boards comprised of non-project, but knowledgeable, engineers that included selected members of the Genesis MIB.

## Sample Return Capsule System Detailed Risk Assessment

The SRC system risk assessment addressed: the SRC battery design, testing, operation and performance predictions; the separation from the spacecraft (cable cuts and separation/spin mechanism function, design, analyses and testing); the AU functions, design and test history; SRC system testing; and testing with the spacecraft. The mechanisms in the SRC were not assessed because their functions were completed with the closure of the capsule after encounter with the comet. The electronics for these mechanism functions were isolated from the entry electronics, although both were housed in the SRC AU.

In the months after the mishap, the Genesis MIB concluded that the Stardust Project could benefit from their preliminary findings, and given some uncertainty on the publication date of their report, developed recommendations for the Stardust Project to address. The full complement of recommendations are listed in Chapter 1; those pertaining to the SRC system effort were:

- Perform destructive physical analysis (DPA) of [the Genesis] flight G-switch
- Evaluate effects of G-switch side load
- Investigate [Genesis] SRC latch operability
- Determine effects of space exposure on seals, vents and science canister filter
- Evaluate Stardust system phasing
- Review Stardust requirements and verification procedures

These recommendations would become another benchmark for assessing the completeness and comprehensiveness of the SRC system risk assessment effort. So much so that the Genesis MIB chair, who participated in selective major reviews during the final year of preparations, would be asked to provide an independent assessment of Stardust readiness at the various institution and agency readiness reviews.

### *Success Tree Approach*

The risk assessment process started from an extensive fault tree that had been developed by the project team during preparation for the comet encounter. This tree was updated and expanded to include all entry faults, an effort described in more detail in Chapter 7. Probabilistic risk assessment tools, in particular event trees, were also employed to help examine and identify critical risk areas. These sources of information were fed into a success event listing, which was prepared to identify all of the functions that had to work correctly to achieve successful EDL. For each required function, the faults that could prevent EDL success were listed and investigated until the team was satisfied that all risks had been identified, and assessed. The non-programmable nature of the SRC design minimized hardware risks, but also allowed little in terms of operational risk mitigations.

### *Sample Return Capsule System Element Risk Assessments*

The next few pages capture the Stardust specific elements of the SRC that were reviewed during the risk review process. Only minor risks were identified and, although the architecture of the future sample return capsule may or may not resemble the Stardust design, these elements are described for illustrative purposes.

#### *Battery*

Each battery was comprised of four lithium sulfur dioxide cells connected in series to provide 12 volts and 6 ampere-hours to run the AU and to fire the pyrotechnic parachute releases. There was one four-cell battery for each string of the SRC electronics, but the two batteries were packaged in one housing. The graph of the battery load and capacity through EDL is shown in Figure 5-1, which incorporated a conservative storage degradation assumption of 3% per year. Depassivation was accomplished by connecting the battery to an 8-ohm resistive load with a current and for a duration established during pre-launch development with the cell vendor (SAFT).

Depassivation, or more accurately de-passivation, refers to the removal, by discharge reaction, of a very thin, high resistance, self-generated layer of material that forms on the surface of the battery's cathode as a result of the chemical reaction between the electrolyte and the anode when the battery is not under load. This layer is characteristic of lithium-based batteries and failure to depassivate results in a voltage and current delay from the battery upon application of a load. The battery temperature was increased to 50°C (122°F) with spacecraft powered heaters, which had been used throughout the mission, to enhance its performance for entry. A nominal current drain assured that the passivation layer would not reform during coast and operation, but since the AU load was insufficient to maintain adequate current, a resistor was added to the circuit and was mounted on the battery where it also helped maintain battery temperature. The battery review included battery experts and identified no significant risks. The review team concurred with heating the battery to 50°C (122°F) and that the depassivation current and time were appropriate.

#### *Sample Return Capsule Cable Cut and Release Signal*

Pyrotechnic cutting of two cables between the spacecraft and the SRC had the potential of creating electrical shorts between wires in the cable bundles. The successful cable cutter tests of flight-like cables performed during development, which included high and low temperature tests, were reviewed by the team and concluded to be adequate. A more robust test could have provided margin by adding wires to the cables. In addition, while during development a wire-to-wire shorting analysis had been performed, it was repeated by both an LMSS engineer and a JPL engineer during the Earth return review process and compared until all discrepancies were resolved. The review found that appropriate circuit protection had been incorporated in the design, avoiding any issues with residually powered signal lines at the time of cable cut.

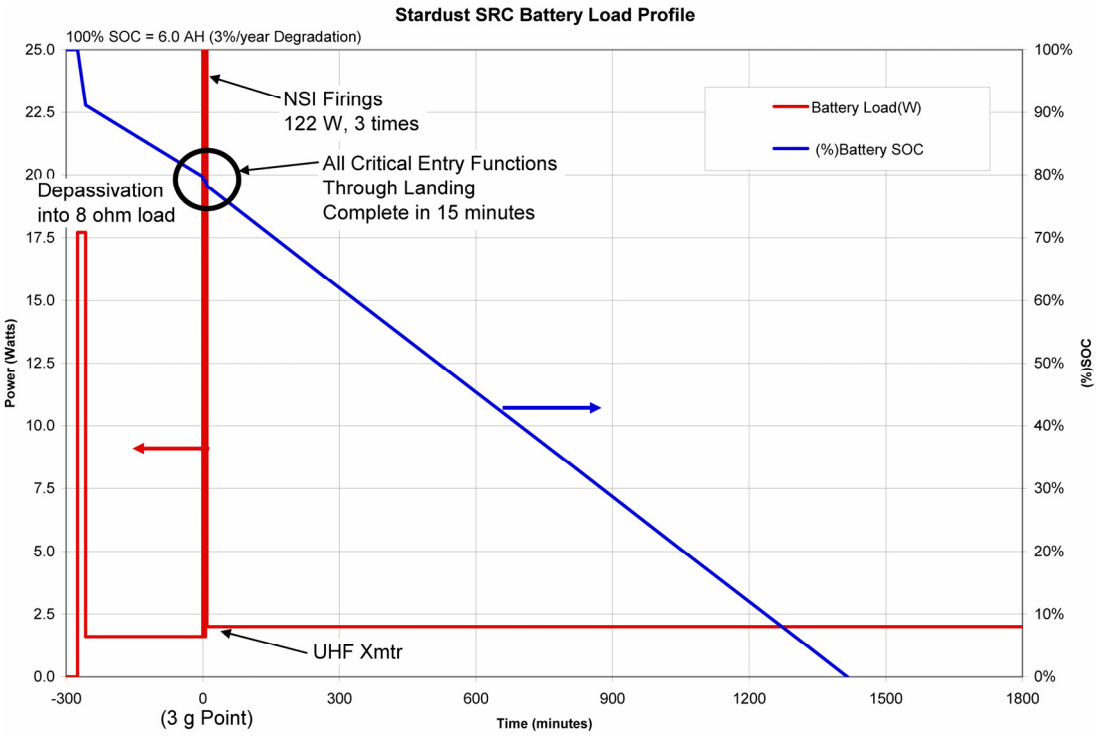



**Figure 5-1. SRC Battery Loads and Capacity**

Nevertheless, to eliminate even this small risk, the spacecraft was configured to stop reading telemetry, thus halting electrical signals across the wires, just before the cable cut.

The pyrotechnic cable cuts and the separation bolt firing were both controlled by the pyrotechnic initiator module (PIM) on the spacecraft. The PIM card had successfully fired the solar array release mechanisms at the beginning of the mission. However, since a single field programmable gate array (FPGA, Actel 1280) controlled both the enable and fire commands, the 'as-built' team identified a risk that could result in Stardust immediately firing the pyrotechnics at PIM turn on, which stemmed from a failure on the Wide-Field Infrared Explorer program that was attributed to a 1280 FPGA that failed high during the turn on. The Stardust PIM card design was analyzed in depth and the development card was tested, verifying that the design of the PIM circuit protected against this failure mode (i.e., 28 volts were not applied until after the FPGA was stable).

*Separation Bolts and Separation/Spin Mechanism*

The SRC was designed to be pushed away from the spacecraft upon firing of three separation bolts on the spacecraft. At SRC mounting to the spacecraft, the separation bolts/nuts were tightened to press three SRC titanium 'cups' against the separation/spin mechanism 'cones'. A concern was raised during the review process as to whether there was potential for the 'cup'-'cone' pair to stick, thus preventing SRC release. The examination verified that dissimilar metals had been used in the design precluding a cold welding issue. In addition, the potential for mechanical interference being the cause of any sticking was analyzed through worst case tolerance build ups and concluded to not be a risk.

The spacecraft separation/spin mechanism was designed to impart a 0.5 meter per second (1.6 feet per second) separation velocity between the spacecraft and SRC, while simultaneously imparting a 13 revolution per minute (78 degrees per second) spin rate. It used three springs for energy storage, and for redundancy, and a cam guide to impart the spin (refer back to Figure 1-2). The mechanism had been extensively analyzed and tested during development in a series

subsystem level tests with a simulated test mass. However, these had been completed prior to the availability of final SRC mass properties. During the risk review process, the dynamic models were updated and extensively run to verify margins for the 'as-built' design, and examine the effects of all plausible failure and worst-case conditions (failed spring, seized rollers, misalignment, etc.). Reviewers concluded that there were adequate margins with the updated SRC properties and failure and worst-case conditions. They also concluded that the mechanism had high reliability.

Due to a change in the Earth return approach attitude plan, including the use of the inertial measurement unit (IMU) for tight deadband control (see Chapter 2), the review team also discovered that the separation/spin mechanism was predicted to run at a hotter temperature than anticipated pre-launch. The IMU was in close proximity to the separation/spin mechanism and generated a great deal of heat. Thermal analysis showed that the flight allowable separation/spin mechanism temperature of 35°C (95°F) would be exceeded to 43°C (109°F). However, the mechanism had been qualified to a temperature of 50°C (122°F) and it was concluded that there was no risk to release. A waiver to the flight allowable temperature was generated and approved.

*Avionics Unit*

The AU specifications, schematics, designs, analyses, as-run test procedures and verification documents were provided for review and analysis to the review team. Their review was followed by extensive discussions with LMSS engineers familiar with the AU, where several operational risks were addressed. The functional schematic of the AU is shown in Figure 5-2.

The first AU event was subsystem turn-on, which was to be accomplished with relay commands from the spacecraft. The potential for relays not working when activated by a single command created a risk that was addressed by the operational approach to issue repeated instances of the relay commands to provide assurance that the relays would close.

The AU was composed of two parallel redundant circuits to sense the deceleration event, issue pyrotechnic device fire commands, and power a UHF transmitter after release of the main parachute. Series redundant G-switches in each redundant circuit were required to be operational to fire the drogue release and the main parachute deployment pyrotechnics. The objective of this design was to preclude any single point failure from prematurely firing a pyrotechnic device while also preventing 'spoofing' of the circuit during atmospheric buffeting (G-switch reopening momentarily causing premature timer initiation). Six degree of freedom aerodynamic trajectory analysis (part of NASA Langley's support of the project) with a simple filter model for the G-switch signal showed about 1 false initiation in 1000 Monte Carlo entry cases. A filter model that more accurately reflected the flight hardware showed that the flight performance would be substantially better. The 1 in 1000 was deemed an acceptable risk during development and the SRC review process reached the same conclusion.

In addition to the G-switch circuit robustness (not to be confused with G-switch robustness, which is discussed later), the timer circuit issuance of pyrotechnic fire signals at the correct time was also verified during development with a worst-case analysis and with flight unit testing. During the SRC review, a JPL electronics engineer performed an independent worst-case timing analysis confirming the timer circuit design. The AU design also provided for main parachute deployment based on ambient pressure – a safeguard against timer failure. This circuit was not enabled until shortly before the time for main chute deployment, but still relied on successful detection of the atmosphere by the G-switches. The review of the AU circuitry confirmed the implementation of this design, but did not delve into the reliability of the barometric switches as other risk tasks took priority.

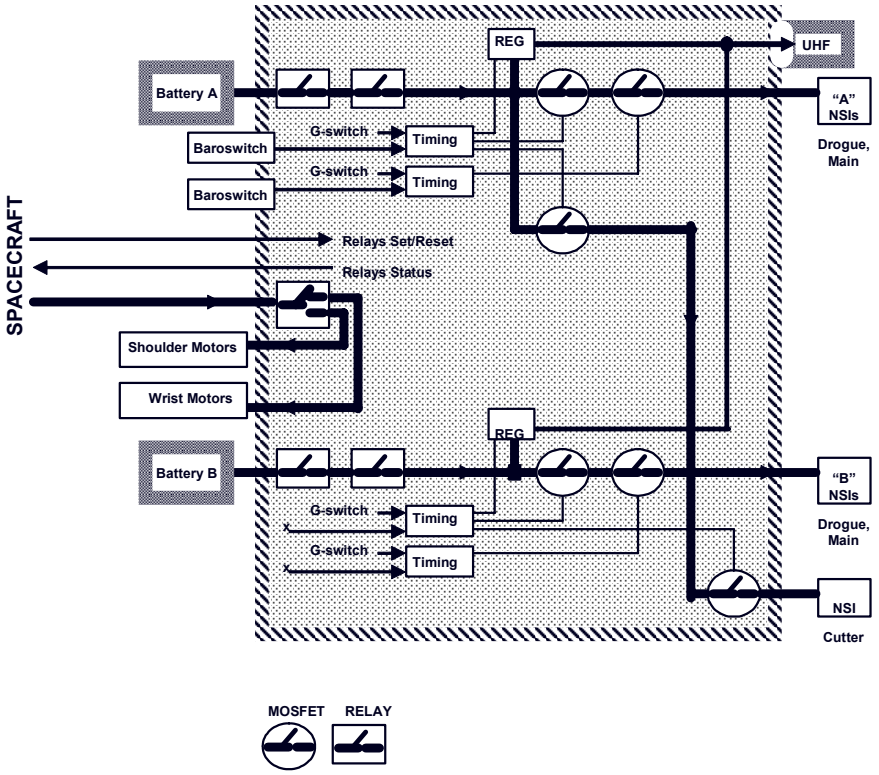



**Figure 5-2. SRC Avionics Unit Schematic**

Upon landing, a 10-G switch was designed to immediately activate a pyrotechnic cutter on the main parachute riser to release the chute from the SRC and prevent dragging the capsule in high wind conditions. This circuit was inhibited until well after main parachute deployment. The main chute had been successfully cut away during a development drop test of a test SRC. These were sufficient to retire any concern over functionality of the device.

During pre-launch pyrotechnic device testing for the Mars Exploration Rovers, a circuit failure was experienced that was attributed to plasma arcing in the initiator which provided a continuing circuit path after firing. Failure investigations revealed that the plasma short could persist for a significant amount of time. Examination of the Stardust AU pyrotechnic circuits confirmed that the design did not include current limiting resistors (the spacecraft pyrotechnic circuits did) introducing the risk that a plasma short in the drogue parachute mortar NASA Standard Initiator (NSI) could pull down the AU voltages to levels (brown-out) that would prevent the AU from performing subsequent pyrotechnic firings (main parachute release and cut away on the ground). While a worst-case analysis of the circuit design showed that this event could occur on Stardust, analysis and tests that included multiple paths to ground showed that the circuit resistance was sufficient to limit the current levels. In particular, the AU circuit made use of metal-oxide-semiconductor field-effect transistors (MOSFET), whose temperatures would rise with an electrical short, increasing resistance, and preventing a sustained plasma short. This analysis was reviewed by the 'as-built' team and the risk review board and accepted as low risk.

In addition to those stated above, the review team meticulously reviewed and analyzed all the AU functions and verified that they would all work as expected. They also reviewed re-work records and verified that proper re-test had been performed. The review team verified correct phasing of all direction sensitive hardware, in particular the G-switches, which is discussed in the next section.

*Deceleration Switches (G-switches)*

Phasing of the Stardust G-switches had been verified during development with a centrifuge test of the flight AU. Additional phasing verification was accomplished by review of close out photos. However, during the investigations by the Genesis MIB, the Genesis G-switches from the flight AU that was recovered intact from the Genesis landing site were tested on a centrifuge. Both G-switches were verified to close within specification, but one switch got stuck in the "closed" position during a 30° off-axis test as the acceleration levels dropped below 3 G's. The switch remained stuck when the centrifuge came to a stop, but a subsequent slight vibration caused the stuck G-switch to open. The MIB recommended retest and DPA of the G-switch that stuck since Stardust was using the same type of switch.

Multiple test runs of the Genesis G-switches again resulted in some instances of switches sticking closed and releasing with slight vibration. A G-switch pulled out of reserve stock was also tested multiple times and also stuck part of the time. The Stardust qualification unit AU (built to flight drawings) was centrifuge tested multiple times during the risk review process and showed some out of specification closure instances and more instances of switches sticking closed. However, these tests were all performed on air-bearing centrifuges with the G-switches in a horizontal position and in a 1-G field, thus producing side loads on the moving mass as it attempted to slide along the wall of the G-switch case.

The G-switches were opened and found to have a small roughness on the mass and the case, which was theorized to produce static friction (see Figure 5-3). Actual measurement of the static friction force at JPL showed that it could be large enough to leave the G-switch closed if there were no perturbations to release the locked parts. To address the side loading concern, subsequent testing was moved to the vendor's facility (Aerodyne). All the G-switches in LMSS stock and some remaining in the vendor's stock were tested on the vendor's centrifuge and all performed within specification. Their centrifuge had mechanical bearings, which introduced small vibrations sufficient to avoid sticking. The vendor also tested the G-switches on a cantilevered beam, applying the acceleration along the axis of the G-switch (no side load), and, again, they all performed within specifications; this was the best test method (see Figure 5-4).

The conclusion of the examination of this risk, concurred by the review teams, was that static friction was the probable cause of the anomalous G-switch behavior and that proper operation of the Stardust G-switches could be expected during the actual entry as a result of significant aerodynamic disturbances.

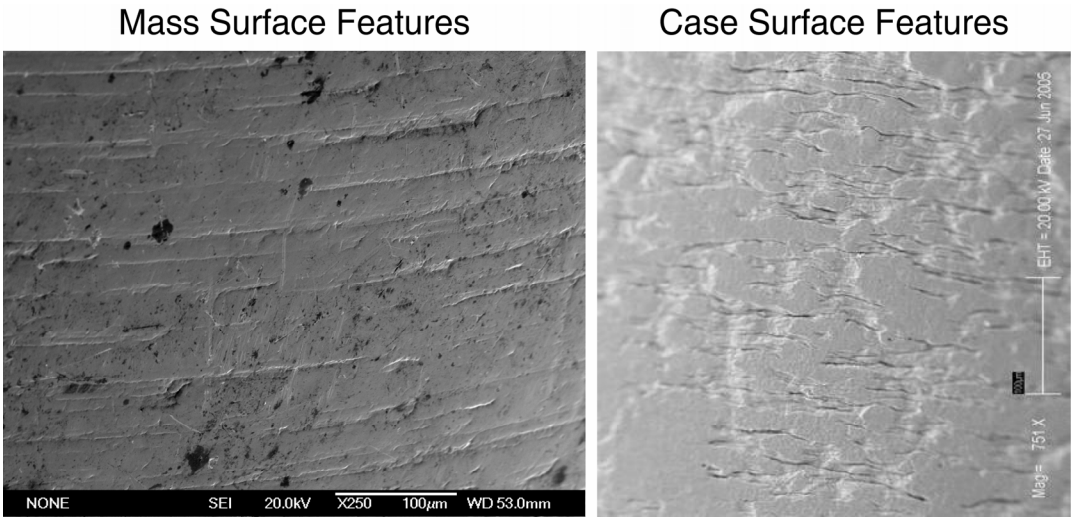



**Figure 5-3. Small Roughness on the Surface of the G-switch Mass and Case**

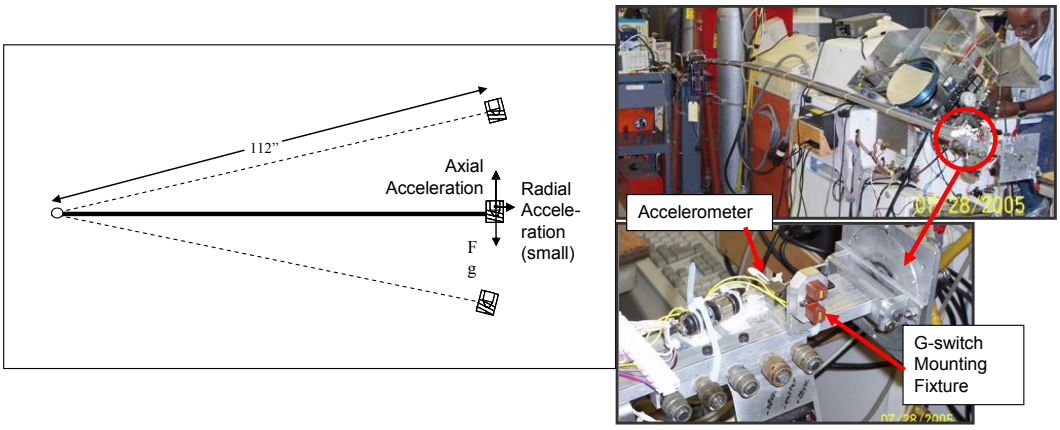



**Figure 5-4. No-side Load G-switch Test Set Up**

*Sample Return Capsule Latch*

One of the three Genesis SRC latches was also recovered from the Genesis landing site in the open position. The Genesis MIB recommended an investigation to determine whether this could represent a risk to Stardust, which was where the latch design had originated. Review of post comet encounter telemetry showed that the Stardust latches were closed by both step count and microswitch indication. The latter would occur only when the latch was driven to the overcenter 'latched' position. Close examination of the Genesis latch revealed that the driven gear was in the closed position and that the mechanical failure occurred due to the hard impact. The other two Genesis latches had not failed but rather pulled the interfacing latch bar out of the backshell on impact. The associated risk to the Stardust return was deemed retired.

*Sample Return Capsule Seals*

The seals between the capsule heatshield and backshell, and around a test connector plug, the push off "cups" and separation bolt cutters were all designed to not allow leakage of hot gasses during entry. Such an event could lead to undesirable heating of the aerogel canister or failure, and breakup and burnup of the capsule itself. Close inspection of the Genesis capsule and the penetration seals showed that there was no degradation of any of the seals and no evidence of hot gas passage. The seal review process, although the Genesis capsule was only in space for 3 years, as opposed to Stardust's 7 years, concluded that the seal materials were not subject to degradation due to long term space storage especially in a benign deep space environment. The risk associated with the sealing designs was judged to be low by all reviews.

*Sample Return Capsule Canister Filter*

A filter was provided on the science canisters of both Stardust and Genesis to prevent ablation gasses from entering the canister during entry re-pressurization. Since the filter was designed during Stardust development, the Genesis MIB recommended investigation of the Genesis filter to obtain any possible insight. Examination of the Genesis debris resulted in the discovery that the Genesis filter had been essentially demolished during impact. Nothing useful to Stardust was learned from inspecting it.

## Challenges in Implementing the Sample Return Capsule Risk Assessment

There was a significant effort required to make all the records available to the Earth return preparation review process, especially for the 'as-built' SRC review. The faster, better, cheaper budgetary constraints imposed during Stardust development resulted in a philosophy to only perform the analyses and testing (with sufficient margins) required to achieve low risk. At that

time, there was no plan or budget set aside for reassessments of analyses and tests during the operational phase, and, consequently, there was no budget committed to special archiving of records. For example, the software for solid modeling of the spacecraft had been upgraded beyond routine backward compatibility and had to go through a significant recovery process to make the SRC solid model available to support the return tasks. Future return missions should plan for archiving that will make all the return and recovery related records readily available.

In addition, personnel with intimate knowledge of the design and test history of all the SRC and spacecraft elements involved in return and recovery were found to be very necessary for the risk review process completed in the months before return. Stardust was fortunate to have almost all of the critical personnel still at LMSS and reasonably accessible. Some exceptions were in the AU designer, who was no longer on-site but fortunately still available for periodic telecons and electronic mail interaction. The separation/spin mechanism designer, on the other hand, was deceased, but the dynamicist who analyzed the separation and participated in the dynamic testing was available to perform updated analyses and guide the review team through the development test results.

By the time of the project-level Risk, Implementation and Certification review, the project found itself with the need to prioritize the work remaining given the funding available to complete the risk assessment and, rapidly becoming more important, the readiness tasks. Sufficient 'as-built' review work had been accomplished by this juncture to suggest the existence of plausible scenarios for off-nominal performance during the Earth return phase. The project's emphasis turned to ensuring that the ground recovery team would be prepared for the range of possible contingency scenarios (See Chapter 10).

External review boards recommended, and the project accepted, prioritizing the remaining tasks, including the SRC review tasks, into three categories: "*1) Priority A—risk mitigation, planning, and operational tasks associated with the nominal Earth return and recovery, plus those off-nominal and contingency tasks related to increasing the probability of achieving a green button return and a safe SRC recovery in the presence of plausible contingency scenarios; 2) Priority B—tasks associated with obtaining risk assessment information that will be of some clear value during the return and recovery phases; 3) Priority C—tasks that yield risk assessment information that will have absolutely no impact on any aspect of the remainder of the mission*." At the project's first Residual Risk review, the SRC system review task was brought to a close with final reporting on the G-switch investigations, the potential for brown-out of the SRC's avionics units due to a short, and the risk of inadvertent SRC release upon PIM card turn on. All of these were felt to fall within Priority B, potentially providing valuable information in the event one of these anomalies occurred.

## Summary of Sample Return Capsule System Risk Assessment

Although the 'as-built' review got off to a slow start as funding took a while to be put in place, the review team was able to spend several weeks to accomplish an in-depth review of the design, analyses and testing of all the Stardust elements that are required for successful return and recovery of the SRC. Review boards were presented with results of comprehensive assessments of the risks, which were all retired or the residual risks were determined to have low or very low likelihood of occurrence. It was extremely valuable to have members of the Genesis MIB participate on the review boards.

Although none of the risks related to the SRC system could be directly mitigated, the information gained during the review process enabled the proper communication of risk posture to the project, and institutional and sponsor community at large. It also enabled the project to identify real-world failure modes that provided the rationale for extensive recovery team contingency planning.

# Chapter 6: Entry, Descent, and Landing System Review

The Stardust Entry, Descent, and Landing (EDL) system review was kicked off in February 2005, eleven months prior to Earth return and five months after the near perfect targeting and entry of the Genesis sample return capsule (SRC) that was followed by a hard landing when its parachutes failed to deploy. The EDL review used assessment methods refined during the Genesis Mishap Investigation Board (MIB) and JPL Failure Review Board joint assessment of, among many other areas, the condition of the Genesis SRC relative to EDL performance. Originally developed in 2003 in support of the Mars Exploration Rover (MER) landing in January 2004, these methods were also used in 2005 for a JPL entry and descent review of the European Huygens probe.

Stardust, like Genesis, utilized a simple entry process and SRC design, which afforded few in-flight risk mitigation options. Nevertheless, the purpose of the Earth return review was to identify and assess the residual risks and possible risk mitigations associated with the SRC EDL. Experience from the Genesis hard landing suggested that risks incurred in a cost-constrained project might not have been completely recognized by NASA management. Stardust was another "faster, better, cheaper" mission that had been completely successful in all operations leading up to Earth return. It was recognized that senior management needed to be fully aware of mission risks, even when few mitigation options existed. For the Stardust SRC, mitigation options were limited to adjusting the entry flight path angle (EFPA) to re-balance risk across EDL subsystems, and diverting to the backup trajectory, not a very viable option for returning the samples. To better understand the EDL risks focused studies and analyses were performed to gain knowledge about risk probabilities and consequences.

The EDL review process covered from SRC separation through EDL. A major focus of the review was the never-flown heatshield material, phenolic impregnated carbon ablator (PICA), the accuracy of its ablation performance modeling, and the adequacy of margins applied to analytic and testing uncertainties in determining the thickness of the heatshield. The review scope did not include operations preparations, SRC tracking, flight operations, separation preparations (except to the extent that risks in these areas affected or invoked EDL risks), or recovery. All of these items are described in other chapters.

## The Team

The EDL risk review team consisted of individuals known to be experts in their respective fields. Many of the team members had been on the MER mission that successfully landed two rovers onto the surface of Mars in January 2004. The MER EDL team experienced significant challenges that were successfully resolved, and this collective experience yielded a risk review team that was able to delve into, and assess the risks of the Stardust EDL. Some members of the team had been involved with the design of the SRC; this intimate knowledge of the system was invaluable. LMSS supported the EDL risk review process as they held key knowledge about the system and the verification and validation program. The lead system engineers of the EDL risk review team were fresh off the Huygens EDL risk review and the Genesis MIB, all of which helped set the stage for a structured, systematic, risk assessment approach.

## Entry, Descent, and Landing Risk Matrix

For the Genesis and Huygens risk review efforts, the review team employed a risk matrix that was populated by enumerating all of the high-level verification items needed to demonstrate that the EDL would be successful. This risk assessment approach was based on a hierarchical "success-tree" methodology that was developed for the MER mission. This was a new way of thinking about verification and validation that was spawned from the view that a traditional requirements-based verification and validation program is considerably incomplete for EDL due to the challenge of enumerating EDL success with requirements. The Huygens and Stardust EDL review efforts utilized this approach to create a risk matrix in order to ensure completeness of the assessment activity. One of the criticisms levied in the Genesis MIB Report was that "red" team reviews can be ineffective if insufficient time is allocated to

complete a penetrating review. Thus, the EDL review was organized to comprehensively identify Stardust EDL risks and to delve into each risk identified in the matrix. In addition, the EDL team reviewed the Genesis MIB draft findings to ensure that EDL-related recommendations that were applicable to Stardust were being adequately addressed.

As the Stardust pre-launch EDL verification and validation program had followed the traditional requirements-based approach, the success tree technique was used to create an independent verification and validation matrix. Each element of the matrix was considered a potential risk until proven otherwise. Research into existing documentation and analyses performed by the review team provided data to determine the degree of residual risk remaining for each element. Figure 6-1 shows the high level EDL success tree structure, where items can continue to be decomposed to the required level of detail. Each "node" in the success tree represents a condition or property that must be satisfied, and forms the basis for one or more entries in the verification and validation matrix, and for the Stardust case, the risk matrix.

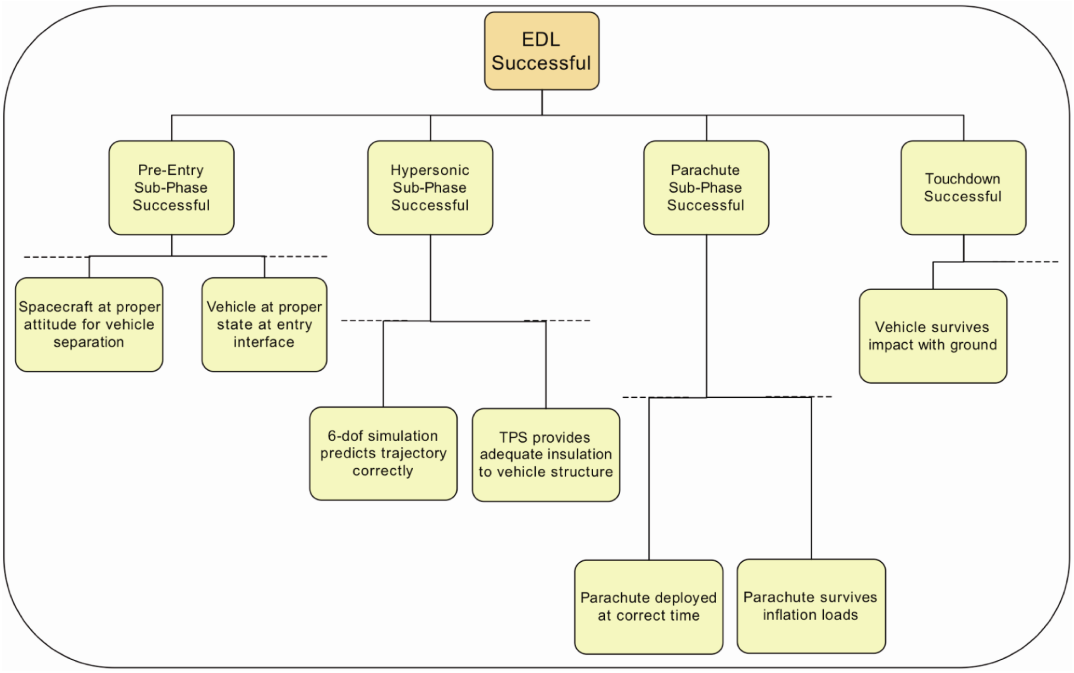



**Figure 6-1. EDL "Success Tree" Structure**

The key EDL subsystems addressed within the risk matrix were simulation and flight dynamics, avionics, parachute descent system, aerothermal environments, and thermal protection systems (TPS). The final risk matrix consisted of a total of 52 high-level risk items. The risk matrix also included an estimated likelihood of occurrence and consequence for each risk item, based on the NASA 5 x 5 Risk Matrix rating system. The EDL team defined the "critical" consequence (5) to be loss of the vehicle and/or the science. For example, this was the rating if a particular risk led to the SRC impacting the ground without the parachute. Likelihood ratings were primarily based on engineering judgment as opposed to rigorous statistical analyses, and the "very high" likelihood (5) was defined as a greater than 10% chance of occurring. These columns within the risk matrix were initially populated by using engineering judgment and by assessing the current state of knowledge regarding the risk item. The ratings were then revised as necessary when new information became available as subsystem focused reviews, analyses, and assessments progressed. Technical details within each of the subsystems were assessed by domain area expert teams from the following organizations:

- Simulation and Flight Dynamics – NASA Langley Research Center
- Avionics – Jet Propulsion Laboratory
- Parachute Descent System – NASA Langley Research Center
- Aerothermal Environments and TPS – NASA Ames Research Center

## Entry, Descent, and Landing Peer Review

An EDL Peer review was held in June 2005, approximately six months before Earth return, and prior to the system-level EDL review scheduled in the review plan. The EDL team felt the addition of this review was beneficial because the quantity and depth of review planned for Earth return by domain experts was not in keeping with the standards that had been established through the MER, Huygens and Genesis MIB experiences. In order to keep the scope within practical limits, the review focused on analyses in the areas that had been designated as residual risks in the risk matrix.

The subsystem areas reviewed were simulation and flight dynamics, aerothermal environments, and TPS. In attendance at the review were EDL experts and critical LMSS Stardust Project personnel. Even though the avionics subsystem was critical to EDL, details were examined within the Stardust SRC 'as-built' review process (Chapter 5). Avionics was an area of heightened awareness and attention due to the Genesis G-switch design error. In addition, while the parachute subsystem was not reviewed at this meeting, a parachute expert from NASA Langley Research Center assessed the design by interfacing directly with the parachute manufacturer and by reviewing design and test documentation. An important aspect of the review process was that the EDL review team chose to interview all of the key subsystem vendors to understand their assessment of residual risk. This was done because of the EDL review team's perception that the "faster, better, cheaper" environment may have prevented people from speaking concerns freely. The majority of analysis and discussion covered in the EDL Peer review occurred in the areas of G-switch reliability, trajectory effects due to the out-of-specification G-switch performance (again, see Chapter 5), adequacy of the aerothermal environment predictions, and heatshield performance and margins.

One of the primary reasons the EDL review team spent significant time reviewing the heatshield performance was to provide NASA management with an independent technical evaluation of the heatshield performance and margins. During this process, the EDL review team found that several misconceptions were present (in 2005) that the heatshield margins were deficient, when in fact the Stardust EDL review team deemed the heatshield design process and margins to be quite adequate. This heatshield element remained a residual risk, however, because it was the first flight of the new, low density PICA, combined with the fact that the SRC entry would be the fastest to date.

Interestingly enough, even though many analysis tools and computational capabilities had increased significantly since the SRC design (especially in the aerothermal area), consistent results were achieved utilizing today's tools as compared with the tools used 10 years earlier. In the flight dynamics area, Genesis trajectory reconstruction provided useful data to build confidence in the tools being used to predict the Stardust SRC trajectory. The margins applied to the several significant uncertainties in the aerothermal and PICA performance modeling were independently and more analytically derived and were consistent with those applied during development. No significant risk items were uncovered as a result of this review, a fact substantiated by subsequent closure of efforts in progress.

## Entry, Descent, and Landing System Risk Review

The EDL Risk review was held in June 2005, two weeks after the EDL Peer review. The objective of this review was to present the residual risks that had been identified during the EDL subsystems reviews and assessments to a broader Stardust risk review team. At this review juncture, the only risk items that were rated "red" (or highest risk) were within the avionics subsystem and were related to the G-switches and the pyrotechnic initiation module that were being addressed by the 'as built' review team. Key residual "yellow" risks included the performance of the PICA heatshield material. Of the 52 total items in the EDL risk matrix, only 50% were rated "green" (or retired risk). In many cases, risk elements were rated "green" out of engineering judgment, as opposed to actual evidence. There were numerous cases where "yellow" ratings were a result of pending analyses that were not completed at the time of the review. Programmatic delays in the start of the risk review activity affected the ability to complete critical assessments and analyses in time for this review. However, at this juncture, there were no risks identified

that would benefit from adjusting the entry flight path angle, nor were there any significant enough risks to recommend the divert backup trajectory mitigation option.

## Entry Flight Path Angle Certification Process

One of the key findings from the EDL Risk Review was that the project had not certified the maximum range of allowable EFPA targets and their uncertainties. This was in keeping with "faster, better, cheaper" practices: a requirement (in this case ±0.08° entry accuracy) was established at the beginning of the development process that all parties could support, which enabled the design effort to make efficient use of resources. During development there had been considerable discussion of the proper balance of entry parameters to maximize the probability of the new heatshield surviving entry (see Appendices G and H). As a result, the SRC was designed to meet capability requirements for an EFPA of -8.2º with errors up to ±0.08° at the atmospheric interface. With concerns about meeting the EFPA accuracy raised by the navigation team and to increase the usage of the approved landing area, the project initiated activities to determine system capabilities at EFPA errors up to ±0.15°, since that was believed to cover the extent of UTTR (see Chapter 4 for discussion of the operational readiness test when, late in the preparation process and too late for EFPA re-certification, it was discovered that ±0.15° did not fully cover the extent of UTTR). Understanding system capabilities at these expanded EFPA errors would assist flight operations decision-making in order to weigh the risks associated with performing the final trajectory correction maneuvers for targeting the desired landing site in the presence of anomalous spacecraft performance. The key EDL system areas affected by expanding the EFPA corridor were aerothermal environments, TPS, the aeroshell structure, and parachute deployment conditions.

NASA Langley Research Center performed numerous EDL Monte Carlo trajectory analyses for various fixed flight path angles (ranging from -7.6° to -8.6°), as well as for expanded errors beyond ±0.08°. A joint NASA Langley, LMSS, and JPL team then evaluated the results to determine if they met all success criteria for the aerothermal environment (i.e. peak heat flux, peak heat load, and stagnation pressure), peak entry deceleration load to the structure, and parachute deployment conditions. Key metrics within the Monte Carlo analyses (3-sigma results), such as peak entry deceleration load, angle of attack at the time of peak heating, and angle of attack at drogue deployment, were still within design and qualification limits. In addition, the SRC drogue and main parachute deployment conditions, such as minimum and maximum Mach number, dynamic pressure, and altitude at deployment were evaluated to ensure these were still within design limits. In fact, there was very little change in any of these key metrics for the ±0.15° EFPA error case when compared with the original design limit of ±0.08°.

Following the Monte Carlo simulations, a few select bounding trajectory cases were developed by LMSS and delivered to NASA Ames to perform high-fidelity computational fluid dynamics (CFD) aerothermal environment analyses. The steep and shallow EFPA bounding cases, combined with a 2-sigma reduction in atmospheric density and the SRC coefficient of drag, were utilized for conservatism. Calculations were performed at multiple time steps along each trajectory for both zero and 10° angle of attack cases. These analyses were used to assess whether acceptable TPS margins still existed, including an assessment on whether transition to turbulence was expected to occur as a result of expanding the EFPA corridor. During development, transition to turbulence was not expected to occur for the ±0.08° EFPA error case, so the TPS was designed accordingly. The CFD analysis showed that there was still no transition to turbulence at ±0.15° EFPA tolerance.

In order to ensure that the forebody and afterbody TPS still provided adequate insulation for the underlying structure, peak heat fluxes (including contributions from convection and radiation) and heat loads were evaluated at key areas on the SRC for both of the bounding trajectory cases. These areas on the SRC were the heatshield stagnation point, the afterbody stagnation point, and the forebody/afterbody TPS interface (main seal location). In addition, the peak heatshield stagnation pressure and shear force at the forebody shoulder were evaluated to ensure the results were still within design and test qualification limits. Since the SRC heatshield was an ablative TPS with expected recession, and thus shape change, an evaluation was also required to determine if these bounding cases caused more recession, more shape change, and subsequently increased aerodynamic instability during entry and

descent. Increased aerodynamic instability could cause parachute inflation problems if the angle of attack at drogue deployment exceeded design requirements.

The aerothermal environment CFD calculations for the ±0.15° EFPA bounding cases showed little difference from the design trajectory used for sizing the thickness of the forebody and afterbody TPS. Therefore, no additional TPS thermal response predictions were necessary. Assessments also showed that there were no adverse affects to the aerodynamics of the vehicle or the parachute deployment conditions. The analyses and assessments performed for re-certification of the SRC for EFPA errors up to ±0.15° showed that the SRC still met all original design requirements.

## G-Switch Reliability Analysis

Another issue that was identified by the 'as built' team during the EDL review was a concern regarding static friction of the G-switch (i.e., the G-switch stuck in a closed state) due to the slight roughness in the moving mass and the switch casing when subjected to side load and very low vibration (which were not flight like conditions, see Chapter 5 for more detail). The G-switch initiates timers that trigger parachute deployments and off-nominal performance could lead to parachute deployment conditions beyond the qualified dynamic pressure and Mach number constraints. In addition, concerns were raised regarding the threshold values for the opening and closing of the G-switches being different from specification (this occurred in the time period when invalid centrifuge testing was being performed).

Using the non-flight like G-switch centrifuge tests results that showed threshold values for opening and closing of the G-switches with larger than specification scatter, numerous EDL Monte Carlo simulations were performed to assess the risks to the entry from observed G-switch performance. Fortunately, the results indicated that the parachute deployment conditions were still within requirements. Subsequent test results using more realistic testing conditions showed that the original design specifications for G-switch performance were fully adequate for the mission (again, see Chapter 5).

## Post-Launch Changes in Technology Knowledge

### *Sample Return Capsule Heatshield*

EDL system technology knowledge increased substantially from the time of the original SRC design, nearly 10 years prior to its return to Earth. Analysis tools also evolved and greatly exceeded those used in the original design. One of the residual risks that remained throughout the EDL risk review process was related to the new, low density heatshield material PICA. Additional design detail for the heatshield is discussed in Appendix G, Vehicle Design. Over a year after the Stardust launch, NASA Ames initiated activities to revisit the PICA computational thermal model, which was used to predict the material response under a given aerothermal environment. This effort was necessitated by a review of the calibration approach used in the pre-launch arcjet qualification program that resulted in Ames management invalidating the PICA test data.. As a result of this effort, which spanned several years, a new PICA thermal model was developed and showed additional robustness over the design-era PICA thermal model. However, because the design-era PICA thermal model was not shown to be erroneous, the EDL risk review team considered both as plausible, and evaluated system margins in both cases.

The new PICA thermal model showed significant robustness, and the design-era thermal model showed compliance with requirements, but with only marginal robustness. The performance of the heatshield remained a residual risk because this was the first "system" test of the heatshield and qualification tests were performed only on small coupons in arc jet test facilities. Although arc jet facilities provide the most flight representative TPS test environment available today, there are significant limitations on realism when compared to an actual flight environment. In addition, uncertainties associated with the computational thermal models cannot be retired without flight tests of an instrumented heatshield or

comparison of the returned Stardust heatshield with the models for recession, pyrolysis depth, etc. (see Appendix G for more thoughts on instrumenting future entry vehicles).

***Aeroshell Structure Thermal Model***

The EDL risk review activities occurred simultaneously with Phoenix Mars Lander design activities, and many Stardust EDL review team members were supporting the Phoenix Project as well. A discrepancy in the Phoenix aeroshell structural thermal model was discovered during the Phoenix EDL Critical Design Review in late 2005, and a check of the Stardust case revealed that this discrepancy existed for Stardust as well. The discrepancy related to a difference in the modeled density of the aluminum honeycomb that structurally supported the TPS (sandwiched between two carbon facesheets) when compared to the actual density of the flight hardware. The density of the aluminum honeycomb within the structural thermal model was more than double that of the actual flight hardware. This was a source of concern because the temperature at the TPS/structure bondline interface was sensitive to the density of the structure. Expected temperatures could increase once this discrepancy was resolved. However, during development, the overall stack of TPS and flight like honeycomb structure was arc jet tested and the models were correlated with the bondline temperatures from these tests. Thus compensation for the error in the conductivity of aluminum honeycomb was achieved by adjusting the overall conductivity of the stack to match test results. Since the thermal resistance of the stack was dominated by the conductivity of the heatshield PICA or backshell Super Lightweight Ablator and the honeycomb facesheets, any error would have a negligible to small effect, respectively, on heatshield and backshell stack conductivity respectively.

LMSS provided a new structure property set that corrected the discrepancy in the honeycomb density for use in new TPS thermal model analyses. The property set included values for density, specific heat, and thermal conductivity for the facesheets and the aluminum honeycomb. Thermal modeling experts at NASA Ames reviewed the property set, and while the methodology appeared sound, questions remained regarding the use of reference values for some properties and values from laboratory evaluation for other properties. Unfortunately, Stardust arc jet test data could not be conclusively used to verify this property set, so parametric analyses were performed to understand the sensitivity of the temperatures to variations in these properties. The analyses confirmed that temperature sensitivity was dominated by the total heat capacity of the facesheet. Re-analysis of the Stardust heatshield thermal performance with the new structure property set yielded an insignificant temperature increase. Therefore, it was concluded that there was negligible risk to the heatshield performance as a whole due to any residual unknowns in the structural thermal model.

## Risk Review Closure

Even though the EDL review team was asked to independently certify the SRC for entry, the team concluded it could not do so based on a lack of information regarding verification of some of the design requirements. One example of this deficit was structural qualification of the SRC under peak entry deceleration loads. In addition, due to funding limitations, the project elected to not pursue an in-depth review of the predictions for the thermal state at entry interface, the internal SRC thermal analysis, or the latching and sealing of the SRC. (Note: The structural verification test was reviewed after completion of the EDL activity by the SRC “as-built” review team and found to be thorough. Review of the SRC latches and seals was deemed by the project to not be high priority because the Genesis MIB had reviewed the Genesis latching mechanisms and seals, which were derived from the Stardust design, and showed that they had performed as expected with no evidence of any gas leakage during entry.)

At the Stardust Residual Risk review in August 2005, the status of the EDL review team’s risk assessments and the top EDL residual risks were reported to the project and review community’s satisfaction. The PICA heatshield performance remained a residual risk for reasons stated above. There were a handful of remaining analyses yet to be completed at this juncture, however there were no risks identified that would benefit from adjusting the EFPA, nor were there any risks significant enough to recommend the divert backup trajectory.

# Chapter 7: Flight Operations

The flight operations segment of the Stardust Project was the umbrella under which mission design and engineering, navigation, spacecraft operations, and mission operations, including ground data systems, and Deep Space Network (DSN) support were all engineered into one seamless unit. Having had the fortune of retaining the core team and operations systems during the better part of its 7-year mission, the flight operations preparation focused, as might be expected, on components unique (or somewhat unique) to the Earth return event: rapid design and execution of trajectory correction maneuvers (TCM), accurate and efficient application of the Earth Targeting and Entry Safety Plan (ETESP) decision criteria, development, validation, and monitoring of the sample return capsule (SRC) release and spacecraft divert command sequences, transfer of information to recovery operations elements, and rapid detection and response to contingencies.

The preparation efforts would also need to address a more classic set of items required in support of critical events: examination of spacecraft performance margins, review of flight history, updates to documentation, validation of ground hardware and software, and development of staffing plans and duty rosters. Finally, the execution of a thorough and comprehensive test and training plan would be essential to achieving and demonstrating flight operations readiness.

Given previous detailed descriptions of the mission design and navigation effort (Chapter 2) and ETESP constructs (Chapters 3 and 4), and the upcoming description of external interfaces (Chapter 9), all of which had strong linkage to and participation from flight operations, this chapter focuses many of its pages on the development of an integrated Earth return flight operations procedure, including detection and response to contingencies, development and validation of critical sequences, staffing plan and duty roster development, and design and implementation of the test and training plan.

## Earth Return Preparation Tasks

Before delving into an overview of the preparation tasks, it is worth recognizing at the outset that one of the primary challenges for flight operations was the juggling of its preparation workload with day-to-day operations. A topic already discussed in Section 1.3, it bears repeating as the flight operations teams, navigation included, were the most affected by this overlap in responsibility. Contrary to more popular approaches, a split team, one part dedicated to day-to-day activity and another dedicated to preparing for the critical event, was not implemented on Stardust except at the middle management level (Mission Manager, Project System Engineering, lead LMSS engineers). Being born during the era of “faster, better, cheaper”, the Stardust flight team was relatively small. Only lead engineers had been full time on the project for the majority of its life, with subsystem support being provided within a multi-mission environment (part time on several flying missions). A concerted attempt was made to minimize activities on the spacecraft to enable subsystem engineers to concentrate on the return preparation effort.

An essential ingredient to the preparation process was participation in the suite of external risk and readiness reviews. The Flight operations risk review was scheduled and conducted after the navigation, ETESP, and SRC release sequence and fault protection reviews (just barely for the last of these, see Chapter 1) in an attempt to provide an integrated description of the flight operations construct. Participation in the system-level Risk, Implementation and Certification review, however, would allow possible risk mitigations to be considered in the larger context of the project wide risk posture. Similarly, the readiness review process would build from subsystem reviews to the system-level Critical Events Readiness Review (CERR), where the integrated flight operations readiness posture would be described. The CERR was preceded by navigation, ground data system, and DSN subsystem readiness reviews.

### *Mission Operations*

To prevent a misunderstanding of the information contained within this section, it is necessary to point out that the traditional definition of the "mission operations system" was designated "flight operations" on Stardust. The Stardust "mission operations team" was comprised of those elements of flight operations that were not mission design, navigation or spacecraft operations (refer back to the project organization chart in Figure 1-9), i.e. they were the conglomerate of ground data systems, DSN scheduling and operations, configuration management, data management, and flight operations engineering. The mission operations team was led directly by Mission Management, who retained the ultimate responsibility of integrating all elements under the flight operations umbrella.

Given that Stardust mission operations was largely in place and functioning in support of day-to-day operations, one of the primary preparation tasks was the development, documentation and implementation of interfaces between flight operations elements and recovery operations. However, so important were these interfaces that an entire chapter of this primer has been allocated to its description and discussion, see Chapter 9: External Interfaces. The residual preparation efforts, described within this chapter, revolved around examination of the existing mission operations construct in the context of robustly supporting the upcoming critical event.

The initial mission operations preparation effort included an inventory of all project documentation (plans, procedures, and interface definitions) with the goal of identifying those documents needing to be developed, those needing to be updated, and those that were usable as is in support of the Earth return events. New developments included the ETESP documents [ref S2-S3], the SRC release operations procedure [ref F10], a decommissioning plan [ref F4], the final installment of the planetary protection report [ref P5], and the many external interface (Chapter 9) [ref F7] and recovery operations documents (Chapter 10) [ref R1 – R21]. Updates would be required for the flight operations test and training plan [ref T1], flight rules and constraints, contingency plans [ref F1-F3], DSN network operations plan, and project anomaly reporting plan [ref F8]. Many pre-launch requirements documents, implementation plans, and mission and spacecraft description documents were found to be either adequately up to date, or functionally replaced by new document developments. An example of the latter was the decision to not explicitly update the mission and navigation plan documents. Instead, the revised mission and navigation strategies were captured in the introductory sections of the ETESP documentation.

Another key element of the system-level mission operations preparation effort was the development of staffing plans, duty rosters and the distribution of personnel in the different mission support areas (JPL operations, JPL navigation, LMSS operations, Utah Test Training Range, United States Strategic Command, etc). Team staffing plans and duty rosters were delegated to team leads, and, while the multi-mission operations environment provided a relatively rich pool of trainable analysts, a challenge would present itself when attempting to provide around the clock coverage of qualified decision makers. The solution to this challenge is discussed later in this chapter.

Cross-population of personnel to the different support areas was done selectively on Stardust to reduce the risk of having to abort the capsule release in the event of catastrophic loss of communications between the remote mission support areas. Communications being particularly important between LMSS (Denver) and JPL (Pasadena), key spacecraft subsystem personnel were sent to JPL (Pasadena), where most of the primary decision makers and the anomaly panel (Chapter 4) were located. In addition, project liaisons were sent to Hill Air Force Base (Mission Control for the recovery team, see Chapters 9 and 10), and US Strategic Command to aid communications during the terminal series of Earth return events.

Ground data systems (GDS) preparations, excluding the external interfaces described in Chapter 9, were perhaps the most straightforward to prepare of the mission operations suite. An important part of the effort would be related to the external interface work in that it was essential

to establish redundant communications paths between flight operations teams, and redundant command, telemetry and radiometric data capabilities during the time-critical phases of the Earth return operation. Preparation efforts would also include facilities, hardware, and software configuration management, including design and implementation of expanded mission support areas. The latter was required at JPL in particular as on-console support had been necessary very infrequently in the Stardust mission operations architecture.

The GDS team supported project and DSN test and training activities, with particular emphasis on voice communications and telemetry display software for flight team members not frequently exposed to real-time operations. Education and coordination of the multiple GDS organizations was essential, including development of return event duty rosters with the purpose of ensuring mission events would not be hampered by infrastructure anomalies. The importance of this aspect of preparations would be exposed during project test and training when a computer network router's behavior would jeopardize the navigation team's ability to timely support the ETESP decision criteria process (see Earth Return Preparation Challenges).

DSN preparations for Earth return would encompass three complementary aspects. The first was the specification and scheduling of required support resources: antenna tracking time, a remote emergency control center (ECC), and use of any alternate (non-DSN) assets. Associated specification of criticality levels would help define required personnel support levels and establish configuration control freezes. The second aspect was a detailed review of support requirements versus capabilities, and attendant support risks. This effort would include the JPL control center facilities, telemetry, command, and radiometric equipment, data capture and transmission networks and infrastructure, operations support plans and antenna site readiness, including a review of historical performance, and, finally, tracking equipment dynamic capability. Despite recommendations to the contrary, personnel test and training, the final component of the DSN preparation effort, was not explicitly included in the project specific operational readiness testing. This was done because the unique DSN activities for the Earth return phase were contingency transfer from a primary antenna to a redundant antenna and/or activation of the ECC. Given their day-to-day involvement in operating the Stardust spacecraft, DSN training of these activities was more efficiently accomplished by only involving the project's real-time controllers, i.e. the project's primary interface to the DSN operators.

### *Spacecraft Operations*

The spacecraft operations effort contained the bulk of the unique Earth return preparation tasks for flight operations. Of utmost importance was the development and validation of the SRC release and spacecraft bus divert critical command sequences. Following closely was the development of an integrated SRC release operations procedure. Supporting these efforts, lead engineers would orchestrate the construction of a basic fault tree and subsystem engineers were directed to examine the Earth return events and environments to characterize performance capabilities (or margins) as compared to requirements.

The development process for the SRC release and spacecraft bus divert critical command sequences received particular attention on Stardust due to a lesson learned on Genesis where changes to the sequences were not implemented because of insufficient time for in-depth (beyond engineering judgment) and comfortable (a fairly subjective metric) implementation and validation. A Stardust release and divert critical sequence had been developed and tested pre-launch with actual flight hardware, but said sequence did not include an auto-recovery capability (another Genesis lesson learned), any provisions in support of the new ETESP decision criteria process, or any allowances for mission success contingency commanding. Trade studies were conducted, and periodically revisited, to determine the amount of time available to accommodate these new requirements as function of sequence exposure to faults (run time) and implications to precursor and follow-on activities. The identified time was then allocated (sometimes overlapping) to address the various new elements: allowed delay time as a function of event (auto-recovery),

time required to detect and respond to propulsive events (ETESP criteria), and time required to detect and respond to failure of a critical release event (mission success).

The validation of the critical sequences was conducted primarily on the ground with use of the spacecraft test laboratory (STL) and detailed independent review at the peer and system levels. A sequence verification test plan was developed, documented and implemented, which included over 20 tests to exercise sequence logic branches (needed in particular due to the addition of the auto-recovery capability), parameters settings, fault protection settings, and robustness to spacecraft anomalies. The test plan also prescribed pre- and post-test meetings, subsystem review, and creation of test or sequence anomaly flags, closure of which was subject to sequence configuration management and regression testing. A detailed test procedure was developed for each STL test and was approved by the test program and spacecraft system engineers.

Parallel examination of predicted spacecraft performance for Earth return focused primarily on the 1-AU thermal environment, end-of-mission margins, and the events and spacecraft configurations particular to the approach navigation plan, release and divert sequences, and subsequent Earth flyby. For example, the attitude control subsystem provided a characterization of the inertial measurement unit (IMU) and star camera performance, and its ability to support the return phase attitude plan, trajectory correction maneuver (TCM) plan (as described in detail in Chapter 2), and pointing requirements for capsule release and divert. Propulsion analysis renewed assessments of thruster performance and propellant margins. The power subsystem would be required to update TCM constraints, solar array and spacecraft battery degradation estimates, and predicted depths of discharge for nominal and anomalous capsule release and divert scenarios, with corresponding survival limits for the Earth flyby solar occultation. Telecom analysis was important in understanding the spacecraft's ability to provide solid communications paths for command transmission, telemetry acquisition, and radiometric data gathering - all critical for the terminal phase of the mission. Thermal analysis identified those components that would be at risk in the 1-AU environment and characterized the proximity of predictions to flight allowable and, where necessary, qualification temperatures. Finally, flight software analysis ensured the computer's processor was not overtaxed, and volatile and non-volatile memory was not over-committed.

Development of an Earth return fault tree, with particular attention to first time events, single point failures, and critical events, played an important role in the identification of risk, and development of the operations approach strategy, fault protection strategies, contingency plans, critical sequence testing, and operations test and training scenarios. The construction of the tree was binned by failure to accomplish a required mission event, i.e. failure to navigate to the atmospheric entry point, failure in the release of the SRC, failure to prevent contact between the spacecraft and the capsule, failure to land the capsule safely, and failure to keep the capsule dry. The internal structure of the tree, however, was fault driven with the fault tree matrix containing entries for fault description, assignee, mitigation approach, verification method, verification documentation, need for risk reduction testing, need for contingency plan development, need for operational readiness testing, and post-mitigation risk ranking.

The engineer that had been responsible for pre-launch requirements verification was designated to lead the fault tree development and counted with the participation of representatives from all elements of the flight operations team. In addition, the fault tree was thoroughly reviewed with non-project personnel, i.e. organization internal experts, who were familiar with Stardust. Originally the tree was to be one topic of the Flight operations review, but due to its importance it was matched up with the fault protection strategy, and critical sequence design in their own detailed review.

The spacecraft performance analysis, fault tree, and critical sequence design naturally helped clarify and establish the required characteristics of the fault protection strategy. However, the overall strategy was additionally guided by programmatic principles unique to the Earth return event: maximize safety to humans and property, including ensuring (read "virtually guarantee")

the execution of the divert maneuver (with or without the capsule attached), and maximize the ability to release the SRC. To ensure execution of the divert maneuver, Stardust implemented two divert sequences. The first ("safe mode" divert) resided in fault protection and had been hard coded into non-volatile memory prior to launch to guarantee that the spacecraft would divert past the Earth (or at least attempt to do so) in the event of an anomaly. The second ("baseline" divert) was designed and optimized for achieving the backup orbit trajectory that had been developed in the final year of preparations. During Earth return, the safe mode divert sequence was actually initialized and left running on the spacecraft from the time of the final TCM, after which the spacecraft was targeted to impact with Earth, through the time of the capsule release enable (green button). Once the enable command was sent to the spacecraft, the safe mode divert was stopped and the release sequence and baseline divert were put into play. The safe mode divert still resided in fault protection in the event of a problem with the execution of the baseline divert.

While public and range safety was the highest priority, maximizing the probability of releasing the capsule was further influenced by a mindset to treat the Earth return event as a single opportunity. This mindset was initially set by an uncertainty surrounding the available backup orbit opportunity, but in the end would have more to do with a limited set of available contingency responses (more on this later). The initial fault protection design approach would be to enable responses (i.e. spacecraft activity) for those faults that required autonomous action to comply with safety requirements or improve the chances of successful release and divert. Fault protection responses would be disabled for those faults where no benefit was found. The fault protection strategy would be revisited as test and training events provided evidence of unintended outcomes. In addition, a detailed parameter review (of both fault protection settings and critical sequence parameters) would be requested and conducted as a result of peer review findings.

The detailed, master flight operations plan for the Earth return phase was captured in the development of the Spacecraft Mission Operations Procedure for Sample Return Capsule Release [ref F10]. This procedure provided the minute-by-minute, task-by-task operational implementation of the project's decision tree from the transmission of command sequences for the capsule release and divert through the reconfiguration of the spacecraft bus after the Earth flyby. The procedure focused on flight team tasks, but appropriately designated when, and how the flight team would interact with the recovery team and external organizations. In addition, this single document captured the bulk of the contingency actions available to the team during the final days and hours of the mission.

The level of detail in the procedure varied as a function of the task being described and whether it was unique to the Earth return event. For example, given the many maneuvers executed during the mission, development of the final TCM was described only to the extent required to establish the function being performed (e.g. produce trajectory solution), the team performing the function (orbit determination team), the specific product produced and to whom it was delivered (trajectory solution, maneuver team, respectively), and the amount of time allotted for completion. Each team would then rely on their internal procedures to specify how each function was completed. On the other hand, for monitoring the execution of the capsule separation sequence, the procedure provided minute-by-minute prediction of events and expected telemetry, and went as far as scripting voice traffic for nominal execution of events. The procedure appendices contained team and project meeting quorum lists, agendas, required support products, and related email distribution lists. Email distribution lists for external product deliveries were also specified in the procedure appendix and were maintained under configuration control. This level of detail may seem a bit extreme, but was found to be very valuable as it provided a single source of information for the entire project to use during the return operation.

### *Test and Training*

The flight operations test and training plan was, in effect, the mechanism via which the project validated the seamlessness of the flight operations Earth return system. As can probably be derived by the discussions in the previous sections, the goal of the test and training plan was to

ensure proper understanding and implementation of flight operations plans unique to the Earth return event: approach TCMs, ETESP decision criteria, monitoring of critical command sequences, recovery operations interfaces, and rapid detection, response to, and communication of contingencies.

The training plan was cleverly constructed to progressively educate and rehearse, prior to formal certification through operational readiness testing. Two operations procedure meetings provided a classroom environment for the teams to examine and ask questions about the new aspects of the Earth return event. These meetings were followed by two on-the-clock, but not time-of-day, rehearsal exercises which provided the teams with their first hands-on exposure to the operational timeline, application of the operational procedure and select contingency procedures, product production and interface hand-offs (in particular to external entities), and use of corresponding software and hardware. Finally, two operational readiness tests (ORT) were scheduled, this time at the correct time of day, with the goal of not only continuing to test the team's maturity with procedures, interfaces, software and hardware, but also to test the ability to support actual scheduled duty rosters, in particular for those scheduled to transition to overnight shifts. Of these activities, two of them, one rehearsal and one operational readiness test, in particular the latter, was coordinated with recovery and external interfaces testing to ensure full end-to-end scenario testing, a very important objective given the multiple organizations involved in the Earth return event.

In addition to these more traditional training exercises, the final component of the test and training plan provided for the opportunity, again in a classroom environment, to explore and ensure proper understanding of the decision tree and the ETESP criteria implementation. Led by the training engineer, these discussion sessions were conducted in a simple question and answer format, but allowed for an in-depth and broad quizzing of the decision makers (primarily) and flight team members.

## Earth Return Preparations: Selective Details

It is prohibitive to include a detailed description of all of the flight operations preparation efforts conducted during the final year of Stardust. While the previous section attempted to provide an overview of said efforts, this section and the next will touch selective Stardust topics that were key developments, required special attention to complete or resulted in interesting debate.

### *Sample Return Capsule Release Fault Robustness*

The simple architecture of the spacecraft and SRC limited the response to a failure in completing a capsule release event to either re-commanding the event or attempting the event on redundant hardware. The auto-recovery logic that was added to the capsule release sequence provided the capability to autonomously re-start the capsule release sequence for those failures or faults that were caught by fault protection and resulted in a safe mode entry. In an effort to be efficient with the fairly limited time available to complete the release events, fault protection was configured such that only one opportunity was allowed for re-commanding before forcing a swap to secondary hardware. Some failure modes could present themselves with no feedback to on-board fault detection systems, and, for those cases, processes and commands were put into the release operations procedure for a ground response. Given the time required to diagnose and respond to the fault stimuli, the ground response was designed primarily to switch to redundant hardware, skipping the option to re-try on primary hardware.

The auto-recovery capability, originally a separate sequence, was merged into the main release sequence as a result of a peer review finding that urged sequence and testing simplification by having only one critical sequence to manage. The merging of the sequences was accomplished by adding front-end logic to the main sequence that evaluated which portions of the sequence could be skipped either because they had already been completed, or because the time allotted

for their completion had been consumed. Sequence labels and completion flags, the latter written to non-volatile memory for preservation across a hardware reset, were added to the sequence structure to allow the front logic to perform correctly. The auto-recovery capability was enabled by modifications to safe mode commands that re-initialized the spacecraft, exited safe mode, and "called" on the release sequence to start again, thus invoking the front end logic.

The simple architecture of the command and data handling subsystem, including flight software, led to the selection of time as the ultimate arbiter of whether a sequenced event was to be repeated. And, the limited nature of the contingency responses invoked a general philosophy of simply trying the failed event again. First, try again with the primary hardware as fault protection processing may have cleared the initial fault. If still unsuccessful, try on redundant hardware. Keep trying until it would be detrimental to range safety to keep trying.

On the front end, the time available to expand the release sequence was balanced with allowing sufficient time for a contingency trajectory correction maneuver (Chapter 2), and the capsule release enable (or green button) assessment processes (Chapter 4). On the back end, time was constrained by the need to provide battery recharge time between the execution of the divert maneuver and the Earth flyby solar eclipse. In addition, the divert maneuver could not be delayed indefinitely as it needed to assure the pre-selected burn magnitude would indeed result in an Earth flyby, and that perhaps in the presence of a fault as well. In most fault cases, the response time available would turn out to be only sufficient for a re-try on primary hardware, followed by a single attempt on redundant hardware. In the final risk assessment, this implementation was judged to be considerably robust.

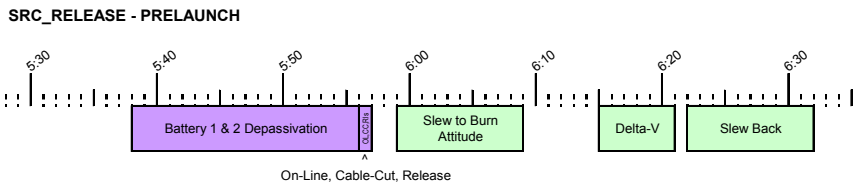
Figure 7-1 shows a comparison between the pre-launch timing of the release sequence and the final return version. The time found on the front end of the sequence was allotted to accommodate the ground processes for the ETESP capsule release disable process (or red button) and parallel ground contingency commanding in the event of a failure to initiate capsule battery depassivation ("command to B-side", see Chapter 5 for further definition of depassivation). The time found on the back end was also allotted to a ground contingency response (again, "command to B-side"), this time in the event of failure to sever the spacecraft harness or failure to activate the separation mechanism. Equally important, this back end time was used to establish the amount of time auto-recovery would allow a particular event to be delayed before it needed to be skipped.

Note that the single opportunity philosophy, described earlier in this chapter, drove the auto-recovery strategy, and overall mission strategy for that matter, to a preference for skipping a release event and proceeding to the next, rather than aborting the release entirely. In this design, the capsule would be diverted with the spacecraft only if the capsule release disable (red button) command had been sent or the capsule physically failed to separate from the spacecraft. For example, in the event of a failure to depassivate the capsule batteries, a prerequisite for the deployment of the descent parachutes, the resulting hard landing was viewed as better than attempting to fly the spacecraft to the backup orbit for another Earth return attempt years later. In addition to the uncertainty about viability of the backup orbit, this philosophy was based on the fact that contingency plans already covered the available response options: re-command and redundant hardware. Why fly another few years when the end result would likely be the same?

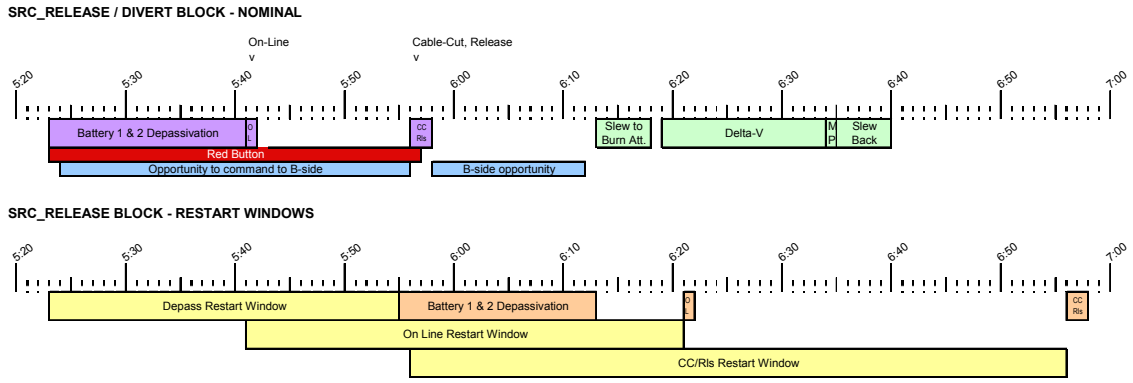
### *Critical Sequence and Strategy Testing*

The SRC release and divert sequence test plan was broken into four specific categories: nominal, auto-recovery, contingency and risk reduction. The nominal tests (3 of them) did not inject any faults and were designed to ensure implementation of the baseline path as a function of outcome from the ETESP enable (green button) process (nominal release and divert, divert only with no preceding release). The auto-recovery tests (9) injected interruptions, either via safe mode entry or heartbeat termination, to the baseline flow and tested all the logic branches within the sequence. To complete the logic test suite, the interruptions were commanded between each

of the major release events in Figure 7-1 (sequence start, battery depassivation, batteries on-line, cable cut, separation, and divert). In addition, logic testing of time-based branches was accomplished by delaying the start of the sequence and following it with the commanded interrupt. Contingency command testing (3) was designed to provide assurances that the key ground contingency commands would play well with the executing sequence. Those selected for testing included implementation of the capsule release disable (red button), and commanded swap to the spacecraft B-side.




**(a) Original Timing**




**(b) Final Construct**

**Figure 7-1. Release Sequence Pre-Launch, Pre-Return Comparison**

The final set of tests, risk reduction tests (14, although only 9 of them would be performed), captured the highest risk faults as identified by the fault tree effort. Several safe mode entries had occurred during the first couple of years of Stardust's flight, the bulk of which were addressed with patches to flight software. The relatively few safe mode entries since then had occurred in the vicinity of extreme solar activity and were believed caused by it. Safe mode entry due to solar activity became the highest credible risk to flight operations. As an aside, in addition to tapping into the national solar weather forecasting media, medium to long-term solar activity forecasts were obtained from JPL resident experts to characterize the risk. Second to the risk of solar activity, the primary IMU and the primary star camera were a couple of the more critical spacecraft components for the return phase. The safe mode risk was well covered in previous testing, so the risk reduction test suite would focus on a failed IMU, failed star camera, and sun coning (an attitude mode response resulting from star camera failure to maintain celestial reference, most likely caused by solar activity as opposed to an actual hardware failure).

Unfortunately, testing of one of the more important aspects of the release robustness strategy, swapping to redundant hardware, was limited by the capabilities of the STL, which actually had no B-side components. The STL's high fidelity simulation of Stardust consisted of flight-spare command and data handling hardware with a workstation interface to simulate the remainder of the spacecraft and the universe. Software simulation of the coupled A- and B-sides had been available prior to launch to relieve schedule and resource pressures during flight software development, but this capability was not retained during operations due to cost constraints.

Resurrection of the dual-side capability was briefly considered to support Earth return preparations, but abandoned due to cost and the conclusion that it would be sufficient to exercise sequence testing through the point where safe mode or ground commands would request the swap to the spacecraft B-side. Validation of the B-side operation was then effectively the same as testing functionality starting from a cold reboot given an appropriate set of initial boot conditions.

There was one flight activity that was available to contribute to the capsule release validation effort. In general, electing to perform an in-flight validation provides the benefit of removing the first order uncertainty regarding basic functionality. Will this piece of hardware turn on and do its job? However, this action must be carefully balanced with the aggregate risk to the mission, what is to be done with the knowledge gained, and the danger of unfounded retiring of risk. For Stardust, the flight activity that was considered was a turn-on of the pyrotechnic initiation module (PIM). The module had not been used since post-launch deployment of the spacecraft solar arrays, and would be used during return to command the electrical harness cable cutters and the capsule separation hardware. Not quite a first time event, but a good 7 years between uses.

Unfortunately, the turn-on event would not provide proof positive that the module was completely operational. To do that, it would need to be exercised to the point of actually issuing the pyrotechnic commands, which obviously was not planned until the actual release event. In addition, if the module were found to not be functioning, the most immediate solution would have been use of the redundant unit on the spacecraft's B-side, but that would have entailed swapping all spacecraft function to the B-side; not a comforting prospect and also an already planned contingency action. The effort was abandoned in favor of simply having access to those redundant hardware contingency commands. As an additional point of interest, perhaps not the driver in the decision, but certainly a consideration, one of the SRC risk assessments (Chapter 5), had identified the very low, but non-zero, probability that the PIM, upon turn on, could fail in a manner that would result in immediate firing of the harness cable cutters and separation nuts; also not a comforting prospect.

***Spacecraft Performance: The moon is WHERE?***

Four areas of concern were identified during the examination of the spacecraft's ability to support approach navigation plans, SRC release, and spacecraft divert. One, the execution of predictable and accurate attitude maintenance and trajectory correction maneuvers, has been discussed at length in Chapter 2. Another, a prediction that the capsule release mechanism temperature would rise beyond its flight allowable temperature, has been discussed in Chapter 5. The third had to do with a shadowing constraint on the solar arrays that might have impacted the execution of TCMs. The last was identified somewhat late in the preparation process and involved discovery that the Moon's location in the night sky, under certain contingency scenarios, had the potential of blinding the attitude control star cameras, unnecessarily jeopardizing the SRC release event.

During pre-launch development, the risk of solar array damage from extended shadowing of selective cells was addressed by the addition of by-pass diodes. Analysis had been completed pre-launch for the shadowed scenario and showed predicted diode junction temperatures were above institutional guidelines but below the manufacturer's maximum allowable operating temperature limit. Accelerated life testing had also been conducted pre-launch to further validate the analysis results. However, no formal waiver to the guidelines had been documented or approved, and examination of mission history revealed that extended solar array shadowing had been avoided in flight. The navigation and attitude control implementation strategy being developed for return required the option of performing slow turns (or attitude maneuvers) for TCMs (to reduce execution errors) and the flexibility for said maneuvers to be fairly unconstrained in direction. To provide this flexibility, the arrays needed to tolerate extended time in shadow (at least several 10s of minutes). In addition, the arrays would need to survive shadowing during a post-divert Earth flyby solar occultation (likely not considered a significant risk pre-launch due to

limited in-depth examination of the Earth return phase and the lack of backup orbit or decommissioning plans). Given the "first time" nature of the possible shadowing events, the project commissioned two independent peer reviews of the pre-launch analysis and testing documentation, with the additional context of the specific Earth return navigation and mission applications. Favorable peer review results allowed documentation and approval of a waiver to the institutional guidelines. The solar array shadowing risk was retired and no corresponding constraint was imposed on the mission.

The discovery of the Moon in the B-side star camera's field of view came as a result of a more detailed examination of the baseline approach and SRC release geometry, which itself was prompted by the realization that the fault protection and contingency commanding strategies were relying heavily on the desire to reach secondary hardware. The secondary hardware of interest was block redundant (not cross-strapped), as were the star cameras, and bringing them on-line would involve commanding a hard reset to the main computer, corresponding loss of attitude knowledge, and reliance on the B-side camera to acquire said knowledge before the release sequence could be re-started. The confluence of these two scenarios had not been anticipated during the development of the fault protection and contingency response strategies. However, those were the correct and proper (and only!) risk mitigation strategies available – the solution would be to move the Moon! Fortunately, the capsule release attitude requirements were only tightly constrained in two of the spacecraft axis (x and y, refer back to Figure 1-2). The third axis was not completely free as altering its direction affected the incidence angle of the Sun on the solar panels and the angular off-set between the low-gain radio antennas and the Earth. A balance was struck between solar power, the telecommunications link, and the location of the Moon in the star camera field of view to enable the release contingency strategy to be retained.

This solution, however, would progressively alter other planned aspects of the mission, illustrating the challenge in and essential nature of comprehensive end-to-end system engineering. For example, the rather straightforward task of changing attitude control calibration plans to reflect the newly selected capsule release attitude was overshadowed by a several kilometer growth in the width of the predicted landing ellipse at the Utah Test and Training Range (UTTR) that the recovery team was using to develop its operational plans. The ellipse, a 99% representation of the possible landing locations, now included mountainous areas and an area of UTTR traditionally off-limits. Recovery operations plans would need to be adjusted.

To be fair, this landing ellipse growth was also due to the TCM error certification effort (Chapter 2) coming to conclusion right about this same time in the preparation schedule. However, that fact probably only helps accentuate the point about thorough system engineering. Another unintended consequence of the bright body solution would present itself during the final few days of operations (not a good time for discovery!) and would entail 10-20 decibel peak-to-peak variations in the telecom signal strength. This event is discussed further in Appendix E.

### *Test and Training*

The test and training plan focused on the period of time from the final design update of the final TCM through the ETESP decision criteria processes, including the possibility of executing a contingency maneuver, and on to the execution of the SRC release and spacecraft divert critical sequences. As mentioned previously, a fundamental part of the training was to exercise the operational interfaces with the external project community (as will be described in more detail in Chapter 9).

The first two hands-on training activities were designated as rehearsals and as a result were not officially graded for the purposes of operations certification. The goal of the first rehearsal was to put the new operations procedure through a nominal execution of the actions described within. Day shift and time jumps were used as appropriate without compromising the integrity of the nominal path. The second rehearsal, however, was designed to force the flight team to respond to a safe mode event immediately following the nominal execution of the final planned TCM.

Occurring at the worst possible time for navigation targeting, the safe mode entry forced the team to juggle diagnosis of and recovery from the safe mode event with design and construction of the contingency maneuver option. A second safe mode event during the execution of the capsule release sequence exposed the flight team to the look and feel of the auto-recovery capability.
The first ORT was geared toward exposing the flight team to actual Earth return duty rosters and unannounced anomalous events. The anomalies were designed to push at the seams that held together the unique elements of the Earth return plan. In addition to parallel implementation of the loss of signal contingency plan, a telecom failure during the execution of the final TCM forced the flight team to address the possibility of needing to execute the contingency maneuver in a scenario initially characterized by a lack of data and later by only a paltry set of data as compared to the expected baseline. A contrived bout with the flu for one of the primary decision makers tested the corresponding transfer of responsibility to backup personnel. And a series of thruster anomalies tested the very foundation of the ETESP decision criteria and led to the addition of a criteria anomaly panel and to a selective change from quantitative to qualitative criteria statements (see Chapter 4 for more detail). The thruster anomalies also went on to exercise new, real-time, thruster performance monitoring procedures and tools, and intra-team coordination (between the navigation and propulsion teams) put into place to support of the capsule release disable decision process (red button).

The final ORT was conducted in conjunction with a full-up recovery operations helicopter drop test and retrieval of an SRC flight spare. This test would constitute the only end-to-end system level test of the project's test program and was extremely important for flight operations due to the changes to the operations criteria and procedures resulting from the first ORT. Once again a standard set of anomalies were introduced: safe mode entries due to solar activity, a telecom load switch failure, a tank temperature sensor failure, and kidnapping of a different decision maker. In addition to the obvious additional testing of the flight team, the timing of the safe mode entries was selected to push on the team's understanding of the decision tree and processes. One particular safe mode event pushed the estimated landing ellipse to the very edge of the acceptable landing area and in the process resulted in the identification of a missing criterion: entry flight path angle (again, see Chapter 4 for more detail). The kidnapping of another key decision maker during this ORT resulted in additional educational briefings regarding the contingency TCM decision processes and criteria.

***The Decommissioning Plan and Final Planetary Protection Report***

The Earth return nature of the sample return mission posed an interesting question regarding the need for formal decommissioning of the Stardust spacecraft bus upon completion of its primary mission. NASA standards for decommissioning are written primarily in the context of Earth orbiting missions with the objective of managing orbital debris in the very busy regions of low Earth and geosynchronous orbits. In addition to orbit capture and decay management, the guidelines also suggest serious consideration be given to draining all sources of energy from a spacecraft prior to end of mission: battery power, propellant load, etc.

Stardust's compliance with decommissioning guidelines was achieved, for the most part, by the hyperbolic nature of its flight trajectory. Assuming a successful divert maneuver, the spacecraft bus would fly past the Earth and enter a heliocentric orbit; no chance for orbital capture. Extreme failures resulting in spacecraft interaction with the atmospheric (either skip out or entry) were considered very low probability and were addressed by the ETESP analysis and documentation. The guidelines for disposing of all sources of energy, on the other hand, came to be at odds with possible future use of the spacecraft in a follow-on mission. As a result, the spacecraft was not drained, but rather placed in a hibernation state to be possibly awoken at a later time.

But, was there a chance of subsequent return to Earth and future creation of orbital debris? What if there was no follow-on mission, what was the nature of the heliocentric decommissioning trajectory? The answer to this question would be obtained, and documented in the Decommissioning Plan [ref F4], by performing sensitivity studies on the divert maneuver

execution and long-term attitude control behavior in the generation of several thousand long-term trajectory propagation scenarios (100 years).

In addition to the Earth impact question, the long-term propagation study looked at the probability of impact with Mars as needed for the final part of the Stardust Planetary Protection Report [ref P5]. The End of Mission report was the final document in fulfilling the planetary protection requirements for the Stardust primary mission. Its objective was to document the disposition of all hardware launched from Earth. The Earth return data was based on the same long term trajectory propagation studies conducted for the Decommissioning Plan, the post-divert reconstructed trajectory state, and the recovery operations status reports pertaining to the delivery of the SRC to the curatorial facilities at the Johnson Space Center.

## Earth Return Preparations Challenges

### *Key Decision Maker Duty Rosters*

The small size of the Stardust team, historically single string, created a rather challenging dilemma when it came to the generation of duty rosters for decision makers. The project's decision tree called for a decision or command approval at entry minus 36 hours, -31.5 hours, -28 hours, -21 hours, -14.5 hours, and multiple decisions from -6.5 to -4.0 hours, the last being the time of capsule separation (refer back to Figure 4-1). In addition to the known decision times, there existed a fundamental need for decision-making capability at any time in response to untoward events.

This schedule was effectively unsupportable by a single person, or even a couple (Project Manager, Mission Manager). In addition, given the criticality of the decisions being made, there was a need to provide qualified backup decision makers in the event a decision maker became unavailable. Furthermore, the Project Manager, who also fulfilled the duty of Recovery Commander (see Chapter 10), had decision responsibility continued into recovery operations. In parallel, the spacecraft bus was being diverted and performing an Earth flyby and also required managerial attention. One of the first strategies employed to address the managerial decision responsibilities was the concept of "one body, one manager". While both Project Manager and Mission Manager were involved in decision making up through separation of the capsule, upon that separation, the Project Manager's responsibility would be to the capsule and the recovery operations. The Mission Manager was granted full responsibility and decision authority for flying the spacecraft bus.

The development of a robust duty roster would benefit from the multi-mission environment at JPL and LMSS. There was sufficient commonality across missions that experienced lead personnel (mission managers, spacecraft leads) from other projects were drafted to cover those portions of the approach timeline and decision making that were more generic in nature (for example, design and build a TCM). Based on 12 hour shifts, the timing of the return events was such that primary (aka "Stardust") personnel could be scheduled during the key baseline events of the approach timeline, while the "second" shift was scheduled during the expected quiet times. Those quieter times, however, could quickly be filled with contingency activity. If the contingency occurred during the previous shift, there was a certain expectation that the primary decision makers would be involved, to the extent possible, in determining the recovery path before ending their shifts. This would then leave the second shift to manage and implement the anomaly response. In some cases, in particular for the contingency TCM, the primary decision makers were scheduled to return to duty prior to execution on the spacecraft.

Providing for backup personnel in the eventuality that a primary decision maker from removed from duty was even more challenging on Stardust. It was accomplished primarily by scheduling duty shift overlaps to coincide with key decision meetings and events at the expense and relatively small risk of a few "officially" uncovered hours during quiet periods of the timeline.

Again, there was an expectation that those times would be quickly covered by expanding duty shifts as needed. The final duty roster for key decision makers was captured in a single chart for the purposes of cross-team coordination. It is shown in Figure 7-2 to illustrate the amount of information captured within and the implementation of some of the strategies discussed above.

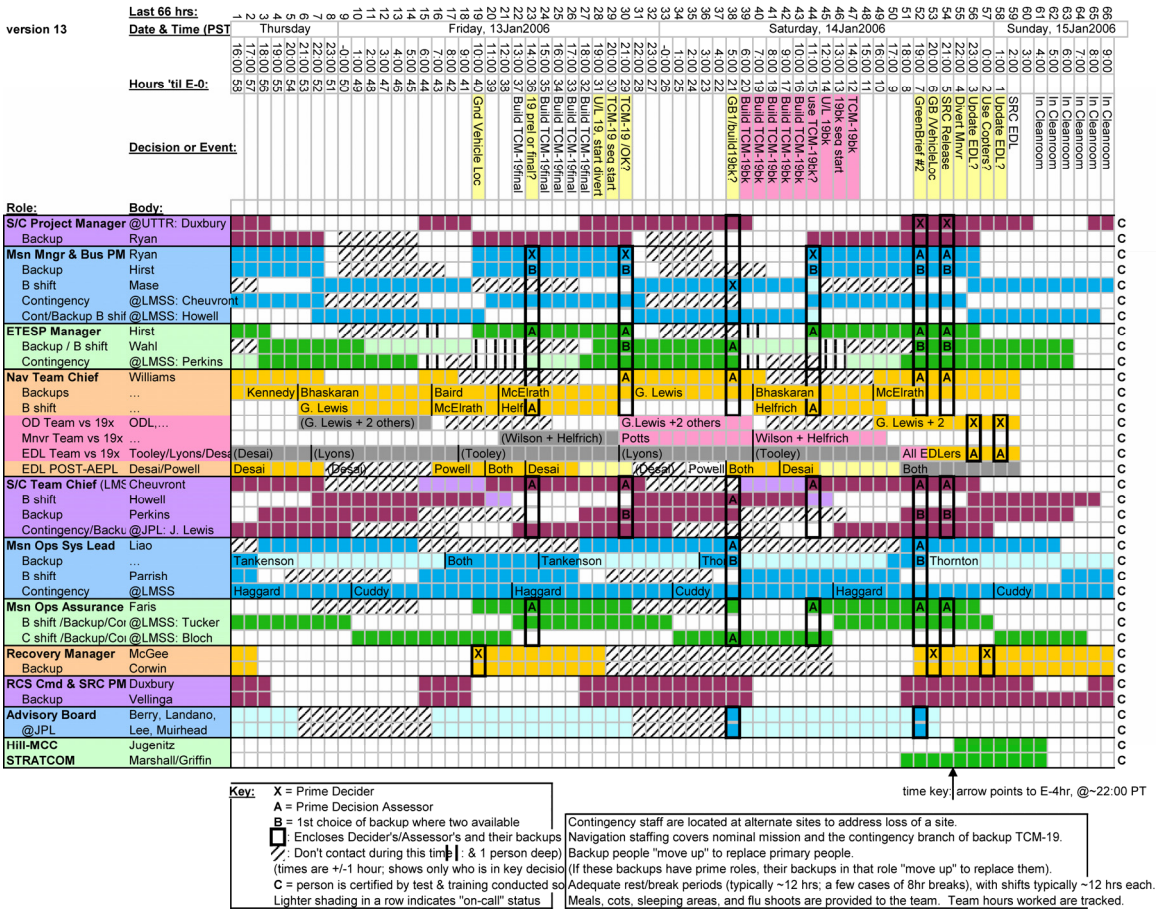



**Figure 7-2. Key Decision Maker Duty Roster**

### *Safe Mode is… GOOD?*

Encompassing navigation targeting in addition to the capsule release events, one of the development challenges for fault protection was identification of when to make changes to settings as a function of mission event. This challenge was in addition to achieving the proper balance between allowing fault protection to take action versus the probability that those actions would create new problems, between implementing new fault protection modes and continuing modes with over six years of flight experience, and between selecting the proper responses to hardware failures versus software failures.

Recalling the discussion of unplanned trajectory perturbations and contingency responses from Chapter 2, safe mode entries within a few hours of the final TCM (at 29 hours from entry) were extremely detrimental to navigation targeting and could result in moving the predicted landing location outside of the approved landing area. On the other hand, for the actual capsule release event, entry into safe mode would have actually improved the chances of a successful release since it was the path to accessing redundant hardware. By this point in the approach timeline, the unplanned trajectory disturbance would have minimal effect (only a few kilometers) on the predicted landing location. The fault protection design was set up to avoid safe mode entries in the former, and was more lenient in the latter.

### *Fault Protection: Command Loss Timer*

The command loss timer was designed to provide protection against the loss of the uplink path between the flight team on the ground and the spacecraft. A countdown timer that was reset upon receipt of a command from the ground, it was a critical component of the fault protection strategy during an event that required critical commanding from the ground. Traditionally, critical event planning and critical sequence development had the goal of eliminating the need for any ground commanding. However, for the sample return mission, NASA range safety requirements established that capsule separation would not be initiated until it was safe to do so. The ETESP construct was designed to be responsive to this requirement and was the very reason for the existence of the capsule release enable (green button) commanding. Obviously, this was a critical uplink that had to exist and had to be protected. Despite traditional goals, the ETESP construct also provided the option to disable the capsule release (red button), another critical command, if safety concerns arose during the execution of the capsule separation sequence. In addition, there was a suite of contingency commands that would, in general, improve the chances of successfully completing the critical event.

The debate over the command loss timer value was somewhat subjective, rooted in engineering judgment of what fault was more likely to cause a loss of the uplink path. Within this debate, the risk balance also included the operational load required to maintain the command loss timer, i.e. how frequently would a command need to be sent to prevent the timer from inadvertent expiration, and the implications of inadvertent expiration, which was entry into safe mode (followed by re-configuration of telecom hardware given enough delay in responding).

The two primary faults under consideration for Stardust's scenario were a failure in the ground data system uplink path and a failure in spacecraft hardware. The latter was judged to be of lower probability than the former given the relatively problem free 7-year flight history of the mission. Together with the consequences of inadvertent expiration, this drove the selection of a minimum command loss timer value of 9 hours, which was representative of the amount of time between the start of DSN contacts. This value provided some protection against ground induced loss of uplink capability while allowing sufficient time for a completely new set of DSN hardware to come into play before the command loss timer would expire.

### *Ground Data System Vulnerabilities*

During the execution of the second ORT, ground network outages severely compromised the ability for the navigation team to complete many of its procedures. The outages were traced to a data router that had been in operation for over 860 days (much longer than typically experienced), and had developed an unanticipated memory usage problem, possibly prompted by first-time testing of high data rates from another project in its pre-launch development phase. Perhaps more importantly, there was no recovery procedure or autonomous failover capability.

With insufficient time to investigate a failover capability, the navigation team developed internal measures to better handle interruption in loss of network traffic. In addition, the GDS team identified critical services and networks in support of contingency procedures to either re-boot hardware or manually move data handling processes to secondary hardware as a function of mission timeline. The event pointed out the complexity of the ground data system infrastructure and the importance of comprehensive risk assessment independent of whether systems had been in use for many years. Stardust benefited from a very serendipitous occurrence of the failure during an ORT to identify and mitigate this particular risk.

### *Fault Tree Development: Risk Rankings*

During the development of the fault tree risk rankings, the original NASA 5 x 5 definitions were found to be too general and not able to fully describe the consequences of the various faults within the tree (also see Chapter 8 for another instance of customization). In particular, the NASA

consequence definitions focused on mission level assessments: (5) mission failure, (4) significant reduction in mission return, (3) moderate reduction in mission return, (2) small..., and (1) minimal…. These were replaced with more descriptive and objective terms appropriate to each Earth return event. For example, the navigation targeting and capsule release mission bins described earlier in the chapter carried the following consequences: (5) failure to completely release the capsule, (4) major targeting discrepancy (off-range), (3) significant targeting discrepancy (>3-sigma), (2) minor targeting discrepancy (>1-sigma), and (1) performs as expected. Similar definitions were applied to the entry, descent, and landing, and recovery operations fault bins.

***The Backup Orbit***

The work done in support of the End of Missions review discussed in Chapter 2 provided the project with the equivalent of an existence proof for a backup return opportunity. In addition to the basic trajectory development, navigation, spacecraft and mission operations assessments were performed only to the extent to show that there were no significant showstoppers to its implementation. The primary backup orbit challenge consisted in determining the amount of workforce to dedicate to the operational development and certification of its validity given the on-going work to assess and plan the primary return opportunity.

One particular challenge was validation of flight hardware life limits. While no significant performance degradation had been detected in flight, pre-launch requirements documentation, as influenced by the "faster, better, cheaper" development approach, addressed component life for only the duration of the prime flight mission - 7-years, no more, no less. Development of additional life assessments would require significant research.

The lack of detailed validation of the backup orbit was particularly difficult to defend in the context of risk posture statements made in defense of the "single opportunity" release sequence and fault protection design choices described earlier in this chapter. These statements were made based on engineering judgment of the work completed during the initial backup orbit development. Furthermore, the priority of the primary mission efforts over the backup orbit development was without question the correct priority.

## Summary

The flight operations preparation effort was marked by a concerted effort to minimize spacecraft activity during the last year of flight thus freeing up the operations teams to participate in the risk assessment and mitigation processes, shore up the understanding and predictability of the spacecraft's behavior, develop and understand Earth return navigation and ETESP decision criteria, generate required procedures and interfaces, develop and validate essential critical sequences, and participate in test and training activities.

The combination of all of these piece-parts into a seamless unit was the result of frequent and thorough communications amongst all partners, including commitment to the risk assessment and readiness review processes. Though not perfect, as test and training and flight events would illustrate, equal value was found in the knowledge gained in preparation for reviews as the knowledge gained from the experience of the review teams.

# Chapter 8: Mission Operations Assurance

The role of mission operations assurance during the sample return phase of the Stardust mission was to provide independent risk assessments to the Project Manager and to the Office of Safety and Mission Success (OSMS) at JPL and NASA Headquarters. The mission operations assurance effort also included a review of JPL Flight Project Practices and Design Principles for residual risks as well as applicability to mission operations, the development of an incompressible test list specific to the sample return operations, and the review of safety and mission success considerations as a result of the Genesis Project lessons learned. Additionally, the mission operations assurance manager provided invaluable insight to the project regarding evolving institutional requirements and expectations in preparation for the return of the sample return capsule (SRC).

This chapter describes the participation of the Stardust mission operations assurance manager in the preparation effort in the context of the extensive detail covered in the previous six chapters. Some of the detail is repeated to illustrate the points being made, but in general the mission operations assurance effort rode in parallel, providing the independent perspective that has already been mentioned. The preparation efforts described herein focused heavily on flight operations, while a separate effort, described in Chapter 11: Recovery Safety, was concerned with recovery operations.

## Preparation Overview

The independent review and assessment of the project's risk posture was performed to facilitate the mitigation of flight operational risks to the sample return operations. This assessment was ultimately reported at the project's Critical Events Readiness Review (CERR), JPL's management readiness review (or Governing Program Management Council Review), and at the NASA HQ Safety and Mission Assurance Readiness Review (SMARR). A SMARR was typically done in preparation for launch. However, the Stardust Earth return was equally critical due to the safety implications of bringing an SRC over the continental United States for landing in Utah. The SMARR was considered to be an essential requirement for Earth return and was conducted in accordance with the NASA HQ Safety and Mission Assurance organization directives.

As part of the project's preparation for Earth return, a series of risk reviews were performed leading up to the previously mentioned readiness reviews. Mission operations assurance independently captured residual risks from these reviews and integrated them into the overall risk assessment. The insight required to complete this task was obtained with active participation in the risk review process and was enabled by becoming an integral part of the flight team. This effort was coordinated with project system engineering as a sanity check and to ensure no identified residual risks had been overlooked. The goal of this process was to get project consensus of the overall risk posture.

The independent assessment effort also included review and assessment of the project's pre-launch residual risk items, in the context of Earth return plans, including single point failures, spacecraft design risks, mission design risks, red flag problem/failure reports, unverified failures, and major waivers. In retrieving the pre-launch information, there was considerable difficulty in accessing the information due to different computer hardware incompatibilities (PC versus Macintosh) and application software upgrades. In the case of Stardust, there was nearly a seven-year interval between launch and Earth return. Projects should ensure pre-launch development information is maintained in an organized and easily assessable format throughout the operations phase of the mission. The historical research also included review and assessment of the project's post-launch incident surprise anomaly database and operational waivers with implications to Earth return.

To characterize compliance with institutional standards, the project's Earth return plans were compared with JPL's Flight Project Practices and Design Principles, notwithstanding the fact that these institutional standards were formalized after Stardust was launched. In particular, institutional requirements established the need for an Incompressible Test List (ITL) to ensure all critical components and sequences were thoroughly tested in preparation for return. The ITL included validation testing in the spacecraft test laboratory along with flight team and ground recovery team operational exercises. An ITL was normally only required in preparation for launch but with the critical nature of the Earth re-entry operations and safety implications, an ITL was developed requiring certain tests be completed prior to SRC return. Non-compliances were risk rated and incorporated into the overall project risk assessment. There were two Flight Project Practices non-compliances in the area of project organization with negligible residual risk for Earth return and 14 Design Principles non-compliances ranging from no to low residual risks. There were no ITL non-compliances.

Mission operations assurance personnel, as members of the flight team, participated in the flight team rehearsals and operational readiness tests (ORT) in preparation for an operational role of providing the Stardust Project Manager with a real-time independent assessment during the Earth return operations that all flight team processes and procedures were being followed. The value of this role and participation in the test and training was illustrated during the second ORT at the second SRC release enable decision meeting. The spacecraft propulsion team criteria for re-entry were being violated (although in further analysis the criteria was found to be too stringent and posed no risk to SRC return). The mission operations assurance manager's recommendation was to not return the capsule and divert to the backup orbit given the pre-approved criteria was being violated. This ORT revealed a situation in which an incorrectly set criterion could cause an unnecessary wave off, placing the SRC into a backup orbit. The result of this vulnerability was the establishment of the anomaly panel and re-examination of the decision criteria construct, as detailed in Chapter 4.

In addition to active participation in the test and training exercises, mission operations assurance worked hand-in-hand with the test and training engineer to verify that the objectives of the training program were being met, and that liens captured were successfully addressed in follow-on exercises. Likewise, during the development of critical sequences, mission operations assurance worked with the test program engineer to ensure compliance with documented test plans and procedures, including proper closure of all liens and anomalies.

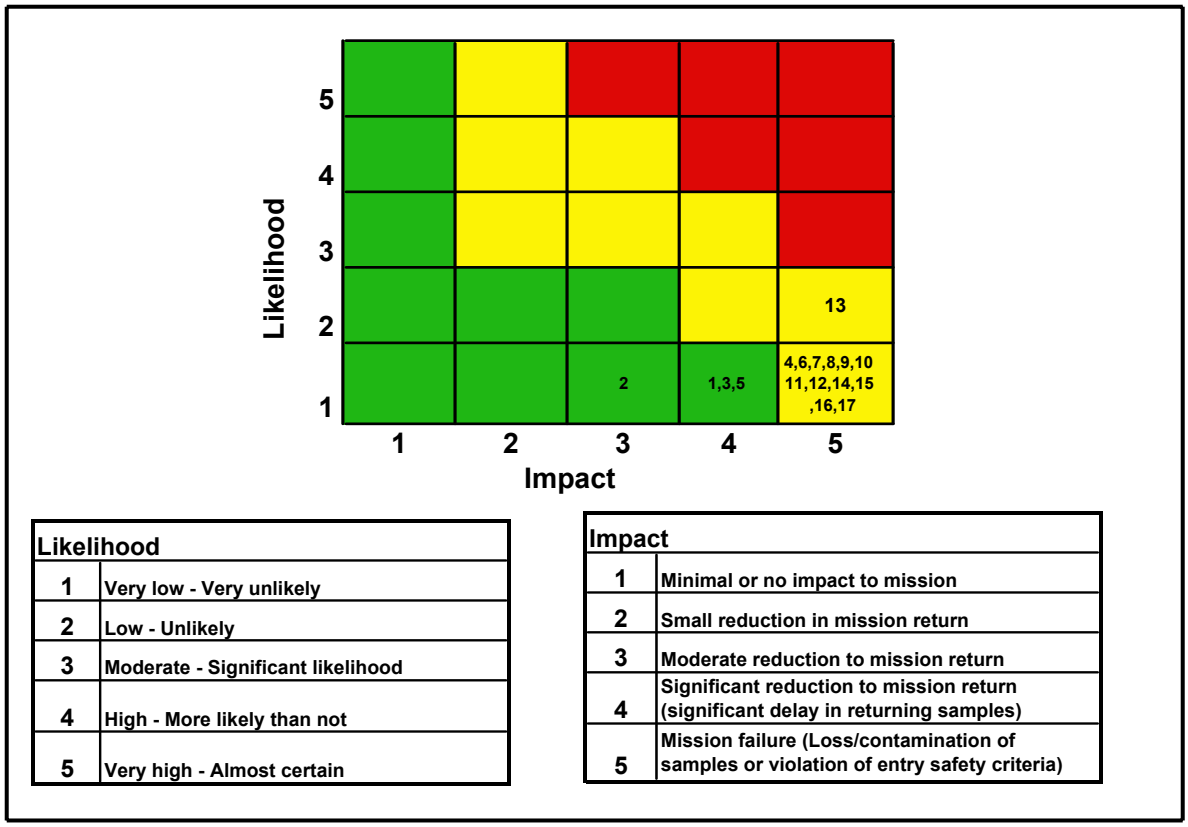
## Risk Assessment

The mission operations assurance risk assessment process was characterized by the placement of risks in one of two categories: those specific to the SRC Earth return phase, and those generic to the entire mission. Several tools were found to be very helpful in the assessment of risk given the tremendous amount of information being generated during the project's eight-month risk process. These tools, illustrated with the specifics of the Stardust Project, are described in the following sections.

### *The 5 x 5 Risk Matrix*

The 5 x 5 risk matrix is a tool used extensively by mission operations assurance managers at JPL to report risk during flight operations. It typically contains the top risk elements out of a more comprehensive list of all project risks. Stardust was only the second application of the matrix to the sample return scenario and the standard ranking definitions were found to be in need of tailoring, much like what was required for the fault tree development described in Chapter 7. For example, mission failure (impact = 5) was redefined to be violation of entry safety criteria and/or loss/contamination of samples as a result of a hard landing, and significant reduction in mission return (impact = 4) was redefined as significant delay in returning samples due to diverting to the backup orbit.

Figure 8.1 shows the Stardust 5 x 5 risk matrix used for Earth return. The x- and y-axes are the standard metrics with the tailored definition of "Impact", as mentioned. The numbers 1 through 17




| Likelihood | |
|---|---|
| 1 | Very low - Very unlikely |
| 2 | Low - Unlikely |
| 3 | Moderate - Significant likelihood |
| 4 | High - More likely than not |
| 5 | Very high - Almost certain |

| Impact | |
|---|---|
| 1 | Minimal or no impact to mission |
| 2 | Small reduction in mission return |
| 3 | Moderate reduction to mission return |
| 4 | Significant reduction to mission return (significant delay in returning samples) |
| 5 | Mission failure (Loss/contamination of samples or violation of entry safety criteria) |

**Figure 8-1. 5 x 5 Summary Risk Matrix for Earth Return**

represented the residual risks identified through the risk management process. Most of the risks had a low likelihood of occurrence but a severe impact, such as loss or significant contamination of science samples.

***Residual Risk List and Example Earth Return Residual Risk Description Summary***

The residual risk list was a tabular description of the risks on the 5 x 5 risk matrix with a brief, one line description of the risk item. The list of risk items was continually reviewed and modified throughout the life of the flight project. The residual risk list shown in Figure 8-2 contains 9 of the 17 residual risks identified for Stardust. The likelihood was judged by the mission operations assurance manager to be very low in 16 of the 17 risk items. The risk rankings were somewhat subjective or qualitative, but the actual numbers were not as important as the discussion of each residual risk and its communication through the management chain. Figure 8.3 is an example of a residual risk description that included the objective rationale supporting the particular selection of impact and likelihood ranking, but more importantly served as a conduit for providing detailed information about a particular risk. Detailed descriptions were developed for all Stardust residual risk items.

| Risk # | Risk Rating | Title |
|---|---|---|
| 1 | 4x1 | Thruster failure causing switch to backup thruster string |
| 2 | 3x1 | Reboot/side swap resulting in unplanned delta V |
| 3 | 4x1 | Spacecraft loss of attitude knowledge |
| 4 | 5x1 | DSN ground station uplink capability lost |
| 5 | 4x1 | DSN ground station downlink capability lost |
| 6 | 5x1 | FPGA in Pyro Initiation Unit (PIU) pyro card fails |
| 7 | 5x1 | Safe mode at end of autonomous sequence recovery window |
| 8 | 5x1 | SRC cable cutters fail |
| 9 | 5x1 | SRC Separation Mechanism (SSM) predicted to be 8 degrees C above flight allowable at release |

**Figure 8-2. Stardust Earth Return Residual Risk List**

**6. FPGA in PIU Pyro Card**

**Description**

- A failure of the PIU FPGA could cause both the enable and fire outputs of a pyro circuit to fail high resulting in a premature firing of the pyro circuit. The failure occurs if all outputs go high or an enable and fire go high on the same circuit. Waiver XF7045 to PRD Requirement.

**Mission Risk**

**Impact: 5** During initial power up of the pyro card in the SRC release sequence (SRC separation - 34.5 minutes), the FPGA SPF causes a premature firing of the SRC separation sep nuts, premature cutting of the SRC cables, and/or premature activation of the SRC battery passivation circuits. This could ultimately result in a hard landing.

**Likelihood: 1** FPGA failure rate is low per MIL-HDBK 217 especially since the Pyro Card is only operational for ~50 minutes during the entire mission. First flight use of the card was during solar array deployment (~15 minutes). Second and last use is required during the SRC release sequence (~35 minutes).

**Figure 8-3. Earth Return Residual Risk Description**

### *Risk Balance Trade Space*

Independent risk assessments of mission trades were also performed in preparation for Earth return. Approximately 9 months prior to Earth return the project reevaluated the baseline nighttime entry versus a daytime entry opportunity, as discussed in Chapter 2. The trade was conducted as a result of the Genesis hard landing and the opinion that a similar event would have been difficult to deal with in the absence of sunlight. As part of the project's review, the trade study information was independently assessed from a safety and mission success perspective. Figure 8-4 contains a summary of the trade study risk drivers as developed by mission operations assurance, which was found to best summarize the risk balance. A "major" risk driver was defined as having a significant impact on human safety or mission success. A "minor" risk driver was defined as not having a significant impact on human safety or mission success but rather an effect on the robustness of the operations. The results were coordinated with and concurred to by the JPL OSMS and accepted as the project position going into the review.

| Risk Drivers | Nighttime | | Daytime | |
|---|---|---|---|---|
| | Human Safety | Mission Success | Human Safety | Mission Success |
| Earth Hazard Avoidance | ++ | | | |
| Ground Impact Hazard Assessment | ++ | | | |
| SRC Design Margin | | ++ | | |
| Ground Station Coverage | ++ | ++ | | |
| SRC processing time - anomalous | | | | ++ |
| SRC processing time - nominal | | | | |
| Backup Orbit Duration | | + | | |
| SRC Release Downlink Data Rate | | + | | |
| STRATCOM Tracking | | + | | |

++ = Major Risk Driver
+ = Minor Risk Driver (More Robust)

**Figure 8-4. Risk Balance Trade – Nighttime versus Daytime Entry**

As an aside, cursory consideration of this trade might lead one to conclude that the daytime landing would be preferred over the nighttime entry. However, the project's recommendation, based on proper balancing of risk, was to preserve SRC aerothermal design margin (more detail in Chapter 2), while accepting the possibility of longer recovery processing time in the event of an anomalous landing.

Mission operations assurance participated in a similar, albeit condensed, trade study done in support of flight operations, one day prior to Earth return. Prompted by a telecom signal multi-path anomaly (more detail in Appendix E), which created large signal strength variations, the trade evaluated whether to stay at the planned high telemetry rate for the execution of the SRC release sequence or to reduce it to improve signal strength and the prospects of telemetry visibility.

## Readiness Certification

The safety implications of the Earth return events drove the development of a readiness certification process similar to that conducted for launch operations. The product of this process was a Certification of Critical Event Readiness (CoCER) document [ref S1], which stated that the project had completed the products, tasks, and reviews required to implement the Earth return. In addition, the CoCER certified that the residual risks to safety and mission success had been identified, documented, communicated and deemed acceptable.

The signature page of the CoCER included the Stardust Project (project system engineer, system contractor, mission system manager, mission manager, systems safety, mission operations assurance manager, project manager, principle investigator), and the Director for Solar System

Exploration (institutional management for the Stardust Project), Chief Engineer (institutional system technical warrant holder), Director of OSMS (institution management), and the JPL Associate Director for Flight Projects and Mission Success (institution management). Figure 8-5 shows the elements of the Stardust CoCER compliance matrix. Note that the project team was responsible for acknowledging and certifying completion of all CoCER items, while the Chief Engineer, Director of OSMS, and the Associate Director for Flight Projects and Mission Success only signed-off on a subset.

**JPL Certification of Critical Events Readiness** (page 2)

**Project: Stardust** **Critical Event: Earth Return and Recovery**

| | Completion of the following tasks and products document the project's residual risk to safety and mission success. X's identify sign-off responsibility. | PSE/MSE | Contr. | MM/MSM | MA/MSS | PM/PI | OCE | OSMS | SM | Remarks (attach additional documentation as needed) |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Functional and performance requirements for complete and minimum mission success (including planetary protection) are documented and are being met | x | x | x | x | x | | | | Recovery Ops Plan signed, SRC Release Operations Procedure signed. Post-divert PP report due 1/31/06. |
| 2 | GDS, DSN and MOS reviews (including performance analysis, mission design, navigation and risk assessment), including action items are closed. | x | x | x | x | x | | | | Done |
| 3 | Flight rules, idiosyncracies, and contingency plans are complete, approved and validated. | x | x | x | x | x | | | | Done. |
| 4 | Post launch waivers (with audit of mod/high risk and dissent by OSMS) and Catl, II ISAs (with audit by OSMS/OCE) are closed. | x | x | x | x | x | x | x | x | Done. |
| 5 | All planned development work needed for the critical event is completed. | x | x | x | x | x | | | | Done |
| 6 | Flight SW and ground SW parameters have been reviewed and test validated | x | x | x | x | x | | | | Done |
| 7 | All safety documents and plans are complete, reviewed and approved. All safety procedures are complete, reviewed, and independently validated. | x | x | x | x | x | x | x | | Recovery Procedure signed, ETESP Volume 1 signed, ETESP Volume 2 signed. |
| 8 | Critical Event Incompressible Test List (ITL) tests (including end-to-end operational readiness tests) are complete, reviewed and any deviations approved by the JPL Director. | x | x | x | x | x | x | x | x | Done |
| 9 | All work-to-go activities from the CERR to the critical event have been planned, reviewed and approved. | x | x | x | x | x | | | x | Done |
| 10 | All CERR applicable Red Flag PFRs have been addressed and dispositioned. | x | x | x | x | x | x | x | | Pre-launch red flags are not an issue. No post launch red flags. |
| 11 | All Genesis MIB issues have been addressed and dispositioned. | x | x | x | x | x | | x | | Letter from MIB chair states all items were addresssed. |
| 12 | All risk review action items and findings are closed. | x | x | x | x | x | | | | Done |
| 13 | Residual risk list for critical event (flight and ground) operations is complete, reviewed and approved by senior management. | x | x | x | x | x | x | x | x | Done |

**Figure 8-5. Stardust CoCER Compliance Matrix**

## Summary

The mission operations assurance personnel on Stardust were effective because they integrated themselves into the flight team, providing value added support in identifying, mitigating, and communicating the project's risks, and providing independent, objective input during test and training and actual flight operations. In addition, the execution of exhaustive investigations into the project's flight and development history and institutional requirements freed up lead system engineers and allowed them to focus on the development of Earth return plans and corresponding risk assessment of those plans.

# Chapter 9: External Interfaces

The previous chapters described the flight operations involved in bringing the sample return capsule (SRC) back to Earth. The chapters that follow describe the many facets of the recovery operation. This is an interstitial chapter describing all the organizations and the handshakes between those organizations, including roles and responsibilities, needed to have a smooth transition between the flight portion of the mission and the recovery operation.

## Key Players

In general, the key players for any mission are assembled during the proposal phase. For both Stardust and Genesis, the "project" consisted of NASA Headquarters (NASA HQ), Lockheed Martin Space Systems (LMSS), the Jet Propulsion Laboratory (JPL) and the Principle Investigator's institution. However, the Stardust (and Genesis) Earth return planning, risk assessment and implementation effort would come to involve many external NASA, government and industry organizations due to the nature of returning a science capsule with extraterrestrial material to Earth. It may come as a surprise to read the list of all the participants that are needed to perform a sample return mission. These partners are summarized in Table 9-1.

**Table 9-1. Key Players and Their Roles**

| | |
|---|---|
| **Stardust Project** | |
| National Aeronautics and Space Administration | Contracting agency, liaisons to federal agencies |
| University of Washington | Principal Investigator institution (for Stardust) |
| Jet Propulsion Laboratory | Project and mission management, system engineering, including range safety assessments, flight operations, including navigation |
| Lockheed Martin Space Systems | Spacecraft contractor, spacecraft operations, recovery operations |
| **Flight Operations Support** | |
| Langley Research Center, Space Systems | Entry, descent, and landing simulations. Also provided expertise for risk assessments. |
| Johnson Space Center, Flight Design and Dynamics | Range safety analysis, in particular risk to humans, property and aircraft. |
| Aerospace Corporation | Range safety analysis, independent assessor |
| **Recovery Operations Support** | |
| Johnson Space Center, Astromaterials Research and Exploration | Sample recovery support, curation and archival |
| Department of Defense: Utah Test and Training Range, Hill Air Force Base, Dugway Proving Grounds | Landing range recovery operations including capsule tracking, and ground logistics support. |
| Vertigo, Inc. (& South Coast Helicopters, Inc.) | Recovery helicopter operations. Also provided test and training facilities in Lake Elsinore, CA. |
| Department of Defense: United States Strategic Command (USSTRATCOM) | Earth approach and entry SRC and spacecraft bus tracking. |
| Ames Research Center, Airworthiness Flight Safety | Independent certification of helicopter flight worthiness |
| **Risk Identification, Assessment, and Mitigation** | |
| Ames Research Center, Space Technology | SRC thermal protection system assessment |
| Pioneer Aerospace | SRC parachute assessment |

## Documentation

When organizations work together there is always some type of work agreement between the parties. Each organization has its own internal and external documents that serve as a vehicle for a formal commitment. The following sections describe the documentation between organizations for supporting

the return and recovery operations. The timing can differ on documentation, that is some of the agreements are required before launch (Memoranda of Understanding, National Environmental Protection Agency approvals) and some documents specific to the return and recovery are generally due some months prior to the actual return date (United States Strategic Command Form 1, Contingency Coordination Operations Plan, Risk Communication Plan). The following paragraphs describe the documents that were required for Genesis and Stardust.

### *NASA Memoranda of Understanding*

As part of the original partnering agreement between NASA HQ, LMSS and JPL two Memoranda of Understanding (MOU) were also signed with Johnson Space Center (JSC) and Langley Research Center (LaRC) for specific services from those centers. While there was no requirement to create an MOU across NASA centers, it was beneficial to establish a common understanding of the scope, schedule and budget requirements. The MOU format was rather informal and it was formally ratified in the Program Operating Plan budgetary process and incorporated in the project implementation and task plans.

#### *NASA Johnson Space Center*

As part of NASA's overall charter, JSC is responsible for the housing and disposition of all extraterrestrial material returned from space. This was mandated by NASA Policy Directive 7100.10D and historically traces back to the housing of the Apollo lunar samples. JSC's responsibilities were broadened beyond lunar samples due to NASA's association with the Antarctic meteorite program and cosmic dust collections with the goal of consolidating the oversight and data management capabilities in one place. The Division of Astromaterials Acquisition and Curation, part of the Astromaterials Research and Exploration Science Directorate, is responsible for overseeing all of the sample collections from Genesis and Stardust.

#### *NASA Langley Research Center*

The MOU with LaRC enabled the project to tap into their expertise in entry, descent, and landing (EDL) simulations, including the very important modeling of SRC aerodynamics and aerothermal exposure, atmospheric conditions, and breakup and burnup scenario propagation. The trajectory simulations were also used to provide pointing angles and associated uncertainties to constrain the search space for Utah Test and Training Range (UTTR) tracking assets.

### *Department of Defense – Use of the Utah Test and Training Range*

Prior to launch, NASA signed a Memorandum of Agreement (MOA) with the USAF Air Combat Command who controlled the restricted airspace over UTTR to secure a landing site and associated support for recovery operations. UTTR is a joint area of operations, with the Air Force controlling the airspace out of Hill Air Force Base, and the Army and Air Force controlling various segments of the ground space via Dugway Proving Grounds. One of the provisions of the MOA was that the USAF would act as the liaison between NASA and the Army at Dugway for the use of range assets. The project had to be sensitive to this joint management architecture. The detailed recovery operations support plans were then documented in a Program Introduction Document (PID) developed by the project, and ratified in a Statement of Capability (SOC) generated by UTTR personnel.

#### *Program Introduction Document – Statement of Capabilities*

Details of the return and recovery implementation were coordinated within UTTR's standard operating procedures for range users. As prospective range users, the project submitted a PID [ref R6] to Hill Air Force Base who acted as the program management office and in turn coordinated participation of the US Army Dugway Proving Grounds who controlled the southern range where the landing footprint was targeted. The PID defined the support requirements desired from the range. UTTR responded with a SOC document [ref R18], which defined how UTTR planned to support the return and recovery

operations along with an estimated cost to the project. A PID-SOC cycle was completed pre-launch to establish the support plan, and cost estimates.

The PID-SOC were updated periodically, in particular during the final Earth return preparations, as required by changes to detailed plans and for specific tests such as a drop test conducted to demonstrate tracking interfaces and recovery operations implementation and training. In addition to the PID-SOC documentation, the UTTR Commander, a military position, was directly involved in authorizing all range operations. The approval process included completion of a Safety Review Board (SRB) process, orchestrated by UTTR, which had particular focus on the safety of the planned operation.

***Department of Defense – Space Surveillance***

Tracking support provided by United States Strategic Command (USSTRATCOM) was covered by an existing, but separate MOA, put into place primarily for launch operations, but broad enough to cover Earth return operations. USSTRATCOM is one of nine unified commands within the Department of Defense (DoD) and is responsible for the operation of the Space Surveillance Network (SSN), which is a network of radar and optical sensors used to track spacecraft and Earth orbiting debris. The details of the requested Earth return support were captured in an Orbital Data Request, known as the Form 1, while USSTRATCOM's response was provided in a Functional Plan.

*The Form 1*

About one year before Earth return, the project prepared and submitted the USSTRATCOM Form 1 [ref R20] to obtain tracking support between the time the SRC separated from the spacecraft bus through the time it was picked up by UTTR sensors. USSTRATCOM support was also desired as a backup to UTTR sensors with the expectation that it could pinpoint the capsule's landing location to within a square nautical mile. The Form 1 contained interface contact information, a brief description of the project, the data being requested, how the data would be used, and the objectives of the support. In addition, the form allowed for specification of a general support timeline, required data accuracies, and data transfer and voice communication methodology.

*The Functional Plan*

After approval of the Form 1, which for Stardust occurred within a couple of months of being submitted, USSTRATCOM generated a Functional Plan [ref R21] to formalize the details of their support. Similar to a statement of work, the Functional Plan was an internal USSTRATCOM document that defined the planning and execution required to ensure efficient, synergistic interactions across a community of military commands, agencies, services, and staff elements. The plan identified specific tracking assets and passes, defined the data products required and generated, and the delivery schedule for these products. It also covered task organization, operations, public affairs, command, control, communications, computer systems, and interagency coordination. An important aspect of the Functional Plan was that it clearly stated that USSTRATCOM and the SSN assets were able to support NASA's scientific interests only on a best efforts basis.

A little known fact was that this document also dealt with ensuring compliance with Article 3 of the 1971 Agreement on Measures to Reduce the Risk of Outbreak of Nuclear War Between the United States and the Union of Soviet Socialist Republics. The SRC re-entered the atmosphere traveling at 12.8 kilometers per second (28,600 miles per hour) and was the fastest man-made object to achieve such a feat. The possibility existed that this event would generate missile launch warnings. This document served to coordinate between USSTRATCOM, responsible for all military operations conducted in space, and North American Aerospace Defense Command (NORAD), responsible for missile event situation assessment.

### *Helicopter Support Contracts*

LMSS was responsible for the selecting the helicopter support contractors for the Genesis mid-air capture and recovery and the Stardust recovery. The use of helicopters was driven by the goal to find the SRC and return it to the clean room hangar (at Michael Army Airfield) as rapidly as possible. Contracting with non-military helicopters was desirable specifically because of the importance of having a solid commitment to support recovery operations that could not be overridden by a higher priority. LMSS contracted with Vertigo Inc. of Lake Elsinore, California to plan and implement helicopter operations because, in addition to their extensive expertise in specialized helicopter operations, they were the only group in the world with recent mid-air retrieval capability, equipment and experience. The original Stardust recovery concept included mid-air capture because of a presumed fragility of aerogel. Later testing determined that aerogel was resilient to landing shocks. However, this resiliency did not exist for the Genesis sample return, and the phasing of both missions engendered a solid working relationship that was maintained through the Stardust recovery.

Vertigo performed all helicopter operations planning, documentation and training, and participated in recovery team training involving helicopter interfaces or operations. Vertigo also took the lead in preparing for and presenting the aircraft operations plans to the NASA Ames Research Center Airworthiness Flight Safety Review Board and Operational Readiness Review Board to obtain approval for the Stardust training and recovery helicopter operations.

Among the specialized operations was the necessity to add ultrahigh frequency tracking equipment, high intensity lights, and an infra-red camera to the helicopters (Figure 9-1). It was also necessary to remove a rear seat to make room for the recovered SRC on its carrying pallet. Vertigo's expertise was essential in examining helicopter options and selection of the AS-350 B2 as the recovery operations workhorse. Vertigo subcontracted with South Coast Helicopters to provide the helicopters, pilots and additional recovery operations support.


**Figure 9-1. Recovery Helicopter Modifications**

In addition to the two South Coast helicopters, a third helicopter was required to transport UTTR security and the rest of the recovery support team. Arrangements were made for UTTR to obtain a UH-60 Blackhawk from the Utah National Guard, but it could be called away at any moment (an event that

actually occurred on Stardust, see Chapter 10), and backup arrangements were made by UTTR for a helicopter from Classic Aviation, a local Utah company.

***Risk Communication and Contingency Coordination Plans***

Collection of fact sheets, project and external conference documents, media training, the development of a risk communication plan, and responses to queries were some of the risk communication tasks completed in preparation for the return of the Stardust samples [ref R11]. The capsule's overflight of populated areas, and the possibility of breakup and burnup scenarios with debris landing outside of UTTR, as described in Chapter 3, also prompted the creation of a contingency coordination document [ref R11] at the federal level. The development of these documents included preparation scripts or templates for press releases to be used by media relations in communicating with the public at large, and organizations and agencies at the local, state, and federal levels. This was quite a time-consuming task for Stardust as a result of the Genesis mishap.

*Review of National Environmental Policy Act Compliance*

The first thing a sample return mission does for National Environmental Policy Act (NEPA) compliance planning is to obtain an Earth return classification from the NASA HQ Planetary Protection Office (PPO). Stardust and Genesis obtained statements of unrestricted Earth return from the PPO in the proposal study phase, which facilitated the project's understanding of what level of NEPA compliance was required. Future sample return missions will be required to have a review by the Planetary Protection Advisory Committee (PPAC) before a classification is finalized. After the preferred landing site was selected, discussions ensued with the organization that controlled the land and air space to secure use of the range at the time of reentry, as described in the previous MOA section. Had a foreign landing site been preferred, an MOA between NASA, the US government, and the foreign government would have likely been required in addition to environmental documentation to meet Executive Order 12114, Environmental Effects Abroad of Major Federal Actions. Likewise, use of privately owned lands or Native American reservations would have also required additional agreements. Use of the Kwajalein Atoll would have required discussions with the Republic of the Marshall Islands and the US Army. Both Stardust and Genesis required an Unrestricted Earth Return Programmatic Environmental Assessment (EA) containing compliance information on the launch and landing sites.

During the final year of preparation for the Earth return, the Stardust EA was subjected to review to ensure currency. This was most effectively accomplished by the institutional group responsible for NEPA compliance (many times also responsible for launch approval) for flight projects and flight instruments, and development of the risk communication and contingency coordination plans.

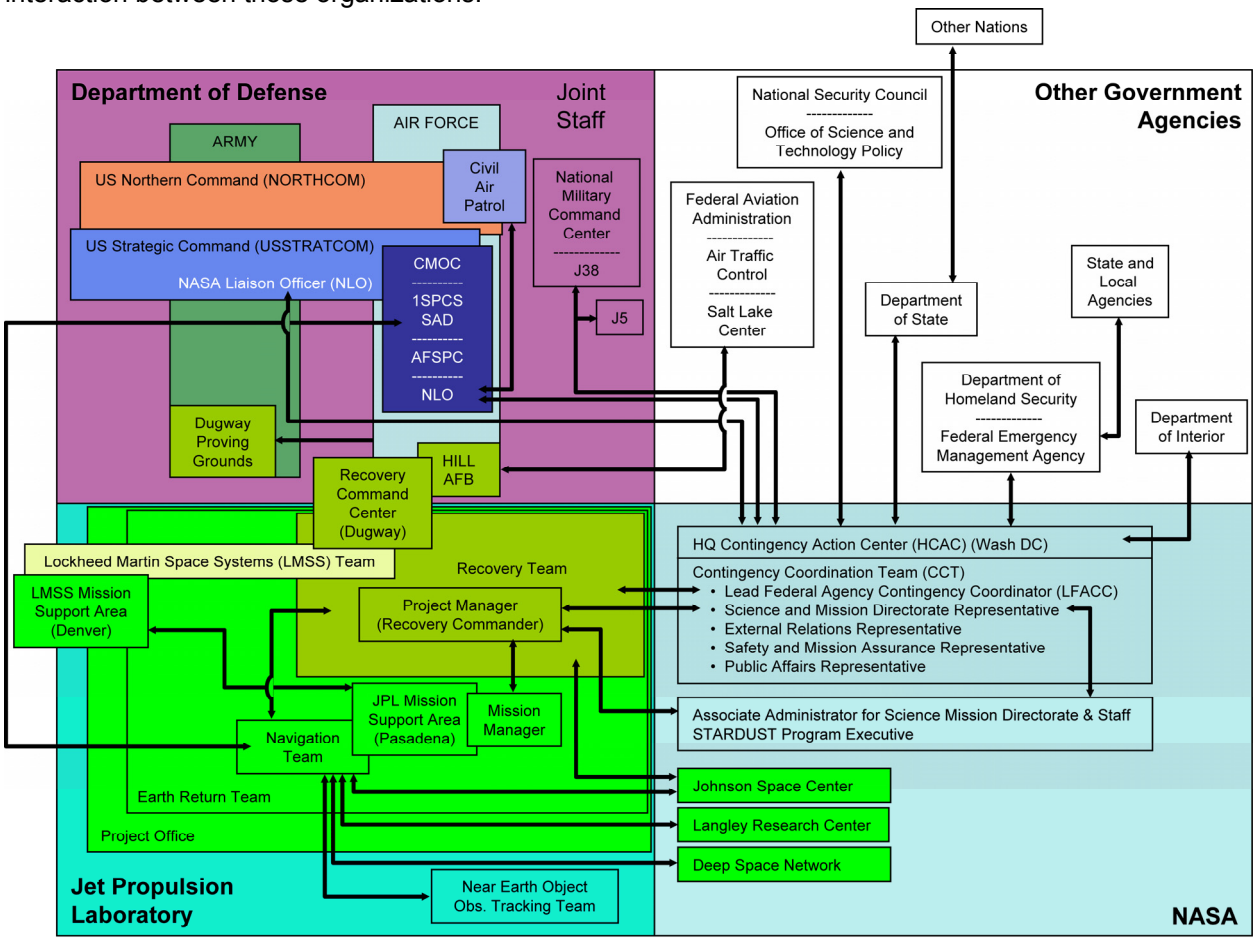
In the event Stardust and Genesis had been designated as restricted Earth returns, current regulations would have required that either the sample be sterilized to the PPO's and the PPAC's satisfaction prior to Earth targeting, or an ability for the SRC to remain intact during a hard landing. In the latter case, additional requirements would have been imposed for the sample to be transported, housed, and contained within a specially designed sample receiving facility with bio-safety level 4-type containment. Certification of the facility, protocols, and trained personnel would have likely involved the Center for Disease Control and possibly other Federal Agencies such as the National Institute of Health, United States Department of Agriculture, etc.

*Contingency Coordination Plans*

Approximately 1 year prior to return, NASA HQ assigned an Earth return contingency coordinator, also known as the Lead Federal Agency Contingency Coordinator (LFACC), who assembled a team that included members from various organizations inside of NASA, including the Office of Safety and Mission Assurance, Public Affairs, International Affairs, and Liaisons to the Department of Defense (specifically various departments within the Air Force), Department of State, Federal Aviation Administration, Department of Homeland Security, Federal Emergency Management Agency (FEMA), etc. The goal of this group was to produce an Earth Return Contingency Coordination Operations Plan [ref R11], which

described the participants, procedures and policies implemented by the Contingency Coordination Team to respond to an off-nominal SRC re-entry.

The primary objective of the plan was to inform and coordinate the actions of the Stardust Project with the actions and responses of teams, organizations, and representatives external to NASA, both internal and external to US Government agencies. It defined the conditions under which a contingency would be declared, the time at which responsibility for contingency coordination would pass from the project team to the Contingency Coordination Team at the NASA Headquarters Contingency Action Center, and when and how contingency response teams external to the project would be informed and brought into contingency operations. Figure 9-2 shows the participating organizations and the lines of communication interaction between those organizations.




1SPCS SAD = 1st Space Command Squadron Space Analysis Division, AFB = Air Force Base, AFSPC = Air Force Space Command, CMOC = Cheyenne Mountain Operations Center, J38 = Joint Staff Space Missile Operations, J5 = Joint Staff Plans, NLO = NASA Liaison Officer

**Figure 9-2. Contingency Operations Matrix**

The Contingency Coordination Operations Plan was also a guide for communicating with other agencies prior to and during the process of anomaly resolution. It established the roles and responsibilities for external communication, provided guidelines and suggestions to effectively answer questions about the mission, what parts were standard, which were difficult, what risks existed, and what mitigations or actions would be taken. As described in Chapter 1, the post Columbia and Genesis climate required several review boards to evaluate plans for operation in Utah. Stardust examined every conceivable entry condition from the moment the Earth was targeted for landing. In all cases the consequence of a failure at Earth entry was deemed high so, for the purposes of contingency coordination, it did not matter that the results of the risk assessments indicated that the likelihood was very small.

For Stardust, a *contingency* would have been declared in the event the SRC was projected to miss the planned recovery site at UTTR, or upon loss of spacecraft control. A *mishap*, on the other hand, was to be declared for those scenarios where alleged or real injury or property damage had occurred as a result of debris striking the surface of the Earth. Breakup and burnup analyses produced in support of the Earth Targeting and Entry Safety Plans (Chapter 3) were extremely useful in communicating risk expectations. Below are brief descriptions of some of the key contingency scenarios as extracted from the contingency coordination documentation.

*Earth Impact within the Utah Test and Training Range Region of Influence*

This scenario was characterized by impact of the SRC and, perhaps (though unlikely), the spacecraft bus onto UTTR or within its region of influence (ROI). This type of contingency would continue to be largely handled by elements of the Stardust recovery team and the UTTR units supporting them. However, it may have required involvement of the Contingency Response Team to notify local civilian authorities through FEMA contacts to identify and secure areas believed impacted by the spacecraft until arrival of the recovery team.

*Earth Impact, Location Known, but outside of the Utah Test and Training Range Region of Influence*

This scenario was characterized by impact of the SRC (or the spacecraft bus) in a known location outside the UTTR and its ROI. Assuming a location interior to the continental United States, this type of contingency would require notification of local authorities through FEMA contacts to identify and secure areas believed impacted by the flight hardware until arrival of the Stardust recovery team. It may have also required use of search assets to confirm estimated locations. The scenario recognized that arrival of the project team could have been delayed by several hours, depending on the distance from UTTR. Impact locations outside of the continental United States would have required coordination with foreign governments through the Department of State in the event recovery operations would have even been attempted.

*Earth Impact, Location Unknown*

This scenario was characterized by suspected impact of the SRC (or spacecraft bus) into an unknown location outside of the UTTR. This type of contingency would have required mustering all of the elements involved in the tracking and analysis of the re-entry with the goal of determining the most likely impact area(s). Once credible areas were determined, and assuming a United States location, search assets coordinated through US Northern Command and the Civil Air Patrol would have been sent out to canvas these areas. Reports from local authorities and citizens would have also been used to determine impact locations. As the previous scenario, identified hardware would have been secured until the arrival of the Stardust team. In addition, search of suspected impact locations outside of the United States would have been coordinated through the Department of State.

One of the trickier aspects of the Contingency Coordination Plan effort was inclusion of the contingency processes in the project's test and training program. The above scenarios were out prioritized by the need to train for higher probability contingencies. However, Stardust managed to complete training of these processes during various off-nominal ORTs, which served as a trigger to set a scenario in motion, and allowed the response to play out in parallel on a non-interference basis with the mainline test.

## Mission Operations

Stardust had to extend the mission operations system during the last six months of the mission to include the ground operations team at UTTR and the support team from USSTRATCOM. For operations in Utah, the ground data systems (GDS) team was solely responsible for setting up and testing Voice Operational Communications Assembly (VOCA) connections to and from JPL, conference lines, secure data server access, and general internet access. VOCA connections and access to data servers were also required from USSTRATCOM. In addition, there were requirements for primary, secondary and tertiary methods

of communication. The biggest lesson that had been learned during the Genesis mission was the efficiency of site visits, well in advance of the critical events and test training, for proper infrastructure assessment and installation.

There were many facilities to deal with for the return and recovery operations in addition to the challenge of being distributed hundreds of miles apart. One example of the distributed operations architecture was the critical SRC release enable polling process (Chapter 4) for Earth entry. The individuals who participated in the decision were located at JPL (Pasadena), LMSS (Denver), and UTTR (Utah), with interested parties passively participating from NASA HQ (Washington, DC) and USSTRATCOM (Colorado Springs and Omaha). In addition, many restrictions existed as a result of operating on military installations, not the least of which was adherence to the chain of command. Computer network restrictions presented a challenge with regard to configuration control and maintenance. One challenge was the discovery that the local network maintenance team was based miles away from the operations sites. Cameras were not permitted in certain locations. Camera phones were prohibited at UTTR unless a special permit was obtained, which were difficult to get. The GDS team spent a significant amount of time learning the policies and local ways of doing business to more efficiently coordinate the required modifications. It was best to assume nothing and coordinate every detail from turning on the heat in a building to scheduling food deliveries. It was very beneficial to define specific points of contact and establish methods of reaching them outside of the daily prime shift hours.

### *Communications*

The voice communications network used for Stardust operations is illustrated in Figure 9-3. The primary communications path while supporting real-time operations was a VOCA net. Remote sites were either equipped with VOCA equipment or used a dial-in capability through normal phone lines. In addition, backup communications were planned through collective conference call capability (known colloquially as meet-me lines), person-to-person cell phone calls, or, selectively, satellite phone calls. With so many external organizations and off-site personnel supporting the SRC return event, it was critical for all teams to be well trained on all methods of communication. As it turns out, this training was accomplished during test and training activities because not all external sites had their primary methods of communication in place. The GDS team made sure that all critical off-site personnel had the same instructions on what to do in case their primary methods of communication failed.

For Genesis and Stardust, there was only one cell phone company providing service to the Dugway Proving Grounds area. Cell phones were an important component of the communications architecture since they provided a backup communications path if land lines failed. However, the control room that housed the Recovery Command System was well shielded, which cut off all cell phone operation. This would not have been known without a site visit. Special antennas had to be purchased so that cell phone reception was possible in the control room and adjacent conference rooms.

In addition to voice traffic, many data files were exchanged using electronic mail. For anything that was mission critical, the subject line included the words “Mission Critical” as an immediate visual cue. However, the risk of loosing electronic mail capability, due to reliance on institutional systems not under control of the project, prompted the acquisition and configuration of a secure file transfer protocol (FTP) server outside the flight operations firewall. Access to the secure FTP server was limited to mission personnel, thus controlling the flow of data. In spite of best intentions, the desired data file transfer procedures were not fully implemented for the Stardust return event. Some of the coordination was slow and unresponsive, and connectivity requirements were not well communicated. The end result was a work around where end users of the data had to rotate shifts and collocate in locations where the protocols had been effectively installed, but that were miles away from their duty stations. Future efforts might benefit from more regular communications, and informational briefings followed by pursuit of commitments further up the local chain of command, beyond those already described earlier in this chapter.

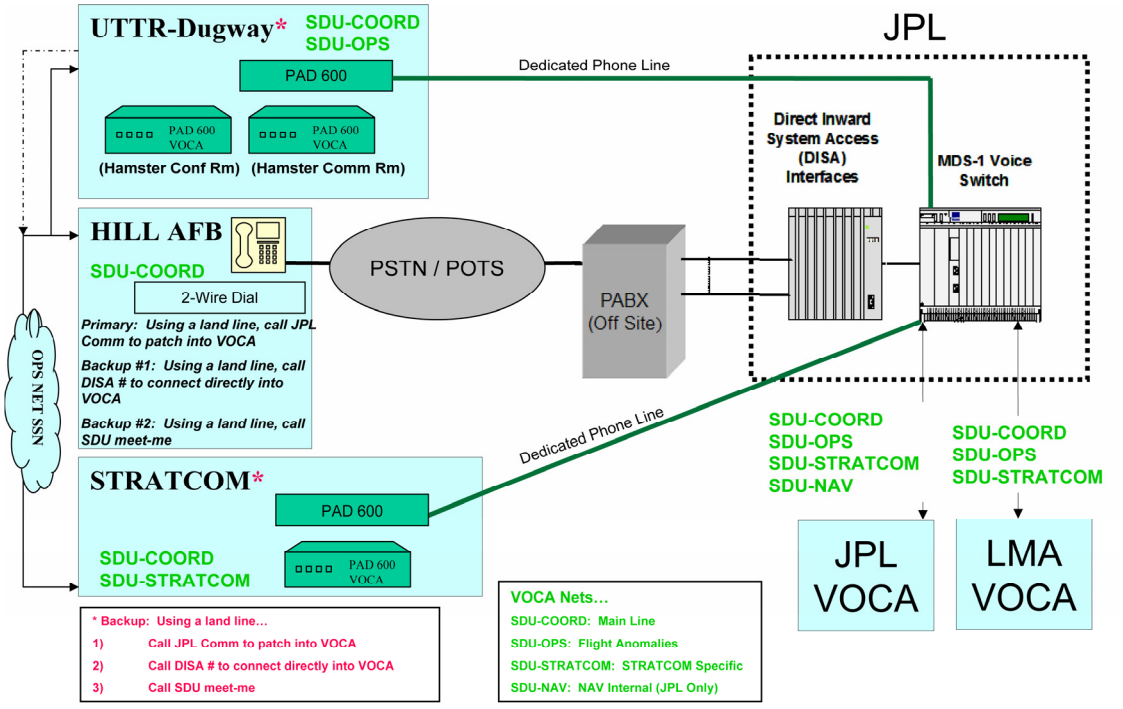



**Figure 9-3 Remote VOCA and Phone Network**

### *Data Product and Interfaces*

In addition to setting up the voice and data infrastructure, it was important to map out the informational products being produced, their content, the producer, the recipient, the production epochs and the intended use. For data products, these agreements were documented in operational interface agreement (OIA) documents [ref F7]. For verbal transfers, the description and logistics were generally captured in operational procedure documents. The information transfer that was planned in support of the Stardust Project is illustrated in Figure 9-4, where the numbered paths refer to specific OIA documentation, and "proc" refers to inclusion in an operational procedure (in retrospect the graphic could have been enhanced by including the actual procedural step).

The bulk of the recovery data interfaces on Stardust addressed transfer of information between the project's navigation team, including the EDL analysts, and tracking personnel at USSTRATCOM and UTTR. The corresponding OIAs specified the contents of navigation trajectory files, USSTRATCOM state vector files, and look angle and search line products for UTTR (for tracking asset pointing). These products are described in more detail below. The data products were transferred via electronic mail and the secure servers described in the previous section, and were aided by the designation of one VOCA channel direct for communication between JPL and Cheyenne Mountain. Allowance for communication with UTTR was granted over the primary project VOCA channel. In addition, a member of the navigation team was located at the USSTRATCOM facility at Cheyenne Mountain as an on-site liaison.

*Data Products Delivered by Stardust Navigation to United States Strategic Command*

In order to enable nominal SSN sensor pointing, as well as nominal and dispersed trajectory analysis by USSTRATCOM, a number of trajectories were delivered to USSTRATCOM by Stardust Navigation. These trajectory products fell into two groups. One group of trajectories was intended for use at

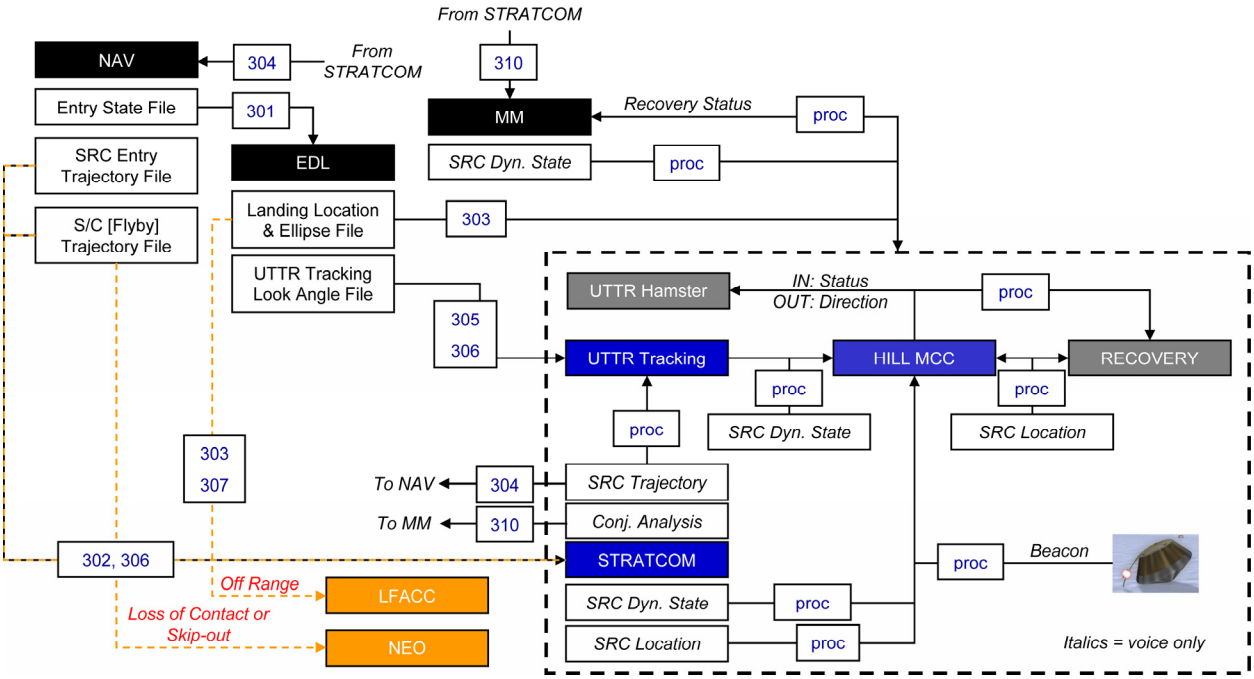



***Figure 9-4. Interfaces for Recovery Data Products***

Cheyenne Mountain to assess SSN tracking capabilities and perform general trajectory analysis. The second group of trajectories was based on the determined orbit of the Stardust spacecraft during the final days of the approach to Earth. In addition to SRC trajectories ending at atmospheric entry, post-separation trajectories for the spacecraft bus were also delivered to USSTRATCOM. The bus trajectories were initialized from the pre-separation trajectory for the two attached spacecraft, at an epoch shortly before separation, and were propagated to one day past the Earth flyby. An additional product, generated by the EDL analysts and delivered to USSTRATCOM, was a trajectory file giving the path of the SRC from atmospheric entry to a time near the deployment of the main parachute.

*Data Products Delivered by United States Strategic Command to Stardust Navigation*

Data products delivered to the Stardust Project by USSTRATCOM were in two forms. The first was a trajectory state vector derived from SSN observations of the SRC. The second was a conjunction analysis performed well in advance of the actual entry to check for close approaches of the SRC and the spacecraft bus to objects in orbit around Earth.

*Data Products Delivered by Stardust Navigation to the Utah Test and Training Range*

To enable UTTR to acquire the SRC during the descent through the atmosphere, the navigation team delivered look angle files for each of the six UTTR sensors used to track the SRC. A seventh look angle file was also provided for a fictitious reference station which was used by UTTR range control to enable coordinated tracking involving different sensors. The look angle files were again generated by EDL analysts based on the propagation of the post-entry trajectory through main chute deployment.

The navigation team also delivered predictions of the SRC landing location. These predictions were used by the recovery team to pre-position the recovery assets and would have been used for actual recovery had the tracking assets not been able to acquire and track the SRC. Landing ellipse predictions were progressively updated in support of the SRC release enable (green button) process (Chapter 4), and upon receipt of actual weather data, just prior to atmospheric entry (Chapter 10). In the event of an anomalous entry resulting in breakup and burnup, the navigation team would have also been the source for debris landing ellipses.

### *Miscellaneous Operations Logistics*

During the Genesis mission it became apparent that some on-site coordination was needed at UTTR. In addition to setting up the distributed ground communication there was facilities coordination and deliveries of hardware, the clean room construction, guest operations, and media interaction that required oversight by project personnel. The addition of a logistics coordinator, to remain on-site at UTTR, partially mitigated this concern, however, it became clear that roles and responsibilities had not been clearly designated. For example, initial duplication of work with the GDS team in setting up internet access led to unnecessary increased cost to the project and confusion with other support personnel.

The environment at UTTR is very isolated and dominated by military activity with food services at Dugway limited to prime shift schedules. During the Genesis recovery activities at UTTR, the team learned that food, coffee and heat needed to be arranged well in advance with the correct department. Stardust benefited from the Genesis experience. It would have been very helpful to have the logistics coordinator handle these arrangements.

As a final logistical note, while military personnel can be a superior resource for staffing, there is a risk of reassignment. For example, the first person selected to be the second helicopter's Director of Flight Operations (see Chapter 10) was pre-empted by duty requirements, much like the Blackhawk reassignment discussed earlier. The Genesis Project suffered from the loss of an Air Force helicopter pilot who participated in test and training, but was reassigned 6 months before Earth return. Likewise, military facilities (i.e., UTTR) may also receive higher priority orders that could have significant impact on the mission. Though unlikely, both Genesis and Stardust projects understood that "events" could occur that would lead to a request to vacate immediately. The lesson that was learned regarding the availability of military assets whether it's a facility, equipment, or people was that it was always subject to the priority as determined by national security. However, both the Genesis and Stardust missions experienced outstanding interagency cooperation and support at every step.

## External Agency Test and Training Support

Coordination of external personnel participation in test and training became challenging on Stardust, in particular with organizations for which Stardust was only one day in an already full calendar. For example, on some occasions, it was difficult to get commitments due to other higher priority military tasks that could pre-empt participation (e.g., on Genesis, a visiting General was considered a higher priority and was a reason for not participating in an operational readiness test). This was another situation where getting commitments from higher in the chain of command, as early as possible, could be beneficial.

## Interagency Advantages

The Stardust Earth return provided two opportunities for engineering and science advancement beyond the direct objectives of the Stardust mission. One was directly beneficial to Stardust, and the other was beneficial to the advancement of entry vehicles. These are described below as additional benefits to non-project entities.

### *United States Strategic Command – Hyperbolic Tracking Capability*

The mission statement for USSTRATCOM is to "provide the nation with global deterrence capabilities and synchronized DoD effect to combat adversary weapons of mass destruction worldwide; enable decisive global kinetic and non-kinetic combat effects through the application and advocacy of integrated intelligence, surveillance, and reconnaissance (ISR); space and global strike operations; information operations; integrated missile defense and robust command and control." Note the emphasis on

protecting the United States from Earth bound attack and one might better understand the focus on elliptical and near-elliptical orbit determination tools and tracking.

The Stardust entry trajectory was hyperbolic with respect to Earth, and absent any additional developments, USSTRATCOM's support role would have been limited to providing measurement residuals against trajectory predictions provided by the project's navigation team. However, the Stardust event provided the catalyst for the development of additional software to process the anticipated measurements and enable hyperbolic orbit determination and prediction capability.

### *NASA Ames Research Center*

The Stardust mission was able to make a contribution to the work at the NASA Ames Research Center for the design of the Crew Exploration Vehicle. As the Stardust SRC entered the Earth's atmosphere it was traveling at 12.8 kilometers per second (28,600 miles per hour). At this speed it was the fastest man-made object to re-enter the atmosphere. The SRC re-entry provided an excellent opportunity for vehicle designers to validate models of convective and radiative heating. As the SRC entered the atmosphere, a team of researchers imaged the event aboard the NASA DC-8 airborne observatory. At SRC entry, the airplane was at an altitude of 11.9 kilometers (7.4 miles) and positioned within 6.4 kilometers (4 miles) of the prescribed, preferred target view location. The incoming SRC was acquired approximately 18 seconds after atmospheric interface and tracked for approximately 60 seconds, an observation period that was roughly centered in time around predicted peak heating. The radiative signal from the SRC and surrounding shock layer gasses were measured by 15 of 18 instruments that had various combinations of spectral range, spectral resolution, and temporal resolution. The data were assessed to be of good quality and sufficient to address all of the observation objectives: absolute radiance, spectral resolution of shock layer emission, and wake train evolution. The post flight analysis was in progress as of publication of this document.

An image from the observation campaign is shown in Figure 9-5. This frame image was published on the cover of the January 23, 2005, issue of Aviation Week and Space Technology and in numerous other publications. The SRC appeared as a bright ball in this optical image, an artifact of saturated pixels blooming into those adjacent. To the human eye, the SRC appeared as a bright point source being bluish early in the entry and then becoming orange-red. Also evident in Figure 9-5 is the trail, or wake train, which was also visible to the eye. The persistence of the train can be related to the rate of chemical processes of the gasses in the wake of the SRC.

***Figure 9-5. NIRSPEC-c IR Spotting Camera on January 15, 2006 9:57:47 UTC***

## Summary

Genesis was the first robotic sample return mission to return to Earth and it revealed requirements, interactions, and interfaces that had been unanticipated or severely underestimated. Much of the work that was accomplished on Genesis was used on Stardust. Future sample return missions now have a model on which to base their developments and operations. Both the Genesis and Stardust missions have paved the way for future sample return missions in their use of UTTR not only because of the engineering work, but also because of the positive and productive working relationships that were developed.

# Chapter 10: Recovery Operations

At 3 am on January 15, 2006 the dark and stormy night cleared briefly for the completion of the second sample return mission in over 30 years. The sample return capsule (SRC) was an engineering marvel, surviving 7 years in deep space, flying through the rock storm of Comet Wild 2's coma and a firestorm return to Earth (Figure 10-1). After a gentle landing in the Utah desert, the recovery team retrieved it and delivered its priceless cargo to an eagerly waiting team of scientists in Houston.

This chapter covers the requirements imposed on the recovery team, the make-up of the team, what operations were performed, what off-nominal recovery scenarios were prepared for, the potential hazards faced and what steps were taken to minimize the risks, and finally the training process that was implemented to ensure all recovery team members were qualified to perform their assigned duties.

**Figure 10-1. Stardust SRC Returns to Earth near Wendover, Utah**

## Recovery Overview

After the Genesis SRC recovery experience, the Genesis Mishap Investigation Board (MIB) recommended that all SRC recovery operations be documented in a single plan and procedure. The recovery operations plan [ref R11] was developed based upon pre-launch requirements and a pre-launch baseline plan with new inputs from safety, quality assurance, the science and curation teams, and range operations experts. The plan specified personnel safety operations, the nominal recovery operation, and credible off-nominal recovery operations. The latter of these, off-nominal scenarios, would be established as those that combined an SRC fault (from the SRC fault tree, dominated by the failure of the drogue and/or main parachutes to deploy) with landing inside the predicted 3-sigma landing ellipse provided by the navigation team (Chapter 2). The Stardust SRC recovery operations procedure [ref R12], a step-by-

step implementation, was then developed from the recovery plan and later updated with lessons learned through the training process. Both of these documents would end up requiring approval signatures of the Stardust Principle Investigator, Lockheed Martin Space Systems (LMSS), Jet Propulsion Laboratory (JPL), and NASA Headquarters managers.

The recovery operations preparations were subject to several independent risk and readiness reviews, as described in Chapter 1. In response to feedback from independent review teams, a project decision tree was generated and the recovery portion was included in the operations procedure to document the recovery decisions required as the procedure was implemented along with who made each decision and what inputs were available to them. In addition, an Independent Review Team (IRT) would be formed to ensure adherence to human safety requirements. While selective challenges regarding accommodating the IRT are discussed within this chapter, the IRT's charter and function are described in more detail in Chapter 11.

### *Operations Background*

Recovery operations started with the release of the SRC from the spacecraft bus and concluded with the hand-over of the sample grid to the Preliminary Evaluation Team (PET) in the Stardust sample curation clean room at Johnson Space Center (JSC). The tracking, locating, recovery, preliminary processing, transportation from the field site to the curation site, and opening of the sample canister were all functions of recovery operations.

For the Stardust mission, the SRC returned to Earth at the Utah Test and Training Range (UTTR) in western Utah. The recovery operations were planned to occur within a 3-sigma downrange and cross range landing footprint of 75 x 25 kilometers (40.5 x 13.5 nautical miles, the black ellipse of Figure 10-2), within the acceptable area of the restricted air space (RAS) of the south range of UTTR (Figure 1-6). A 4.6-kilometer (2.5 nautical mile) buffer zone was implemented around the RAS boundaries and only aircraft supporting the Stardust mission were allowed inside the RAS during the entry and recovery.

The landing target (center of ellipse) was optimized to minimize rugged terrain (mountains, foothills), and low-lying areas susceptible to shallow standing water and mud from rain. In addition, the landing target was located away from the inhabited areas of Dugway Proving Grounds, consistent with meeting range safety requirements (Chapter 3) and SRC release enable criteria (Chapter 4). The location and size of the landing ellipse was very important as the staging of the recovery helicopters and ground vehicles would be based upon this error ellipse. As an additional consideration, entry, descent, and landing (EDL) sensitivity analyses had shown that the SRC would fall within this same error ellipse in the scenario where the SRC's parachutes failed to deploy.

Late in the development of the flight operations strategies, the estimated landing ellipse grew from 75 x 25 kilometers to 75 x 44 kilometers (40.5 x 23.8 nautical miles, larger red ellipse of Figure 10-2) jeopardizing the niche within which the smaller ellipse had fit. However, the project made no change to the landing target, or recovery operations plans due to the low probability of actually landing in the outer regions of the expanded ellipse, the progressive increase in knowledge of the actual landing ellipse, 48 x 20 kilometers (25.9 x 10.8 nautical miles), by the time of capsule separation (4 hours from entry), and the general requirement that the recovery team be able to recover the capsule anywhere within the approved landing region. The footprint fit nicely between the Deep Creek Mountains on the western part of UTTR, Wild Cat Mountain on the north, Granite Peak on the south, and Wig Mountain on the east.

After entry into the Earth's atmosphere, the SRC trajectory remained above 30 kilometers (98,400 feet) until the SRC was over UTTR. A drogue parachute was deployed at 32 kilometers (105,000 feet) above mean sea level (MSL) to stabilize the SRC, followed by the main parachute, deployed at 2960 meters (9,716 feet) MSL, to decelerate the SRC and provide a gentle landing descent rate of 4.6 meters per second (8.9 knots) at touchdown. When the impact of landing was sensed, a cutter severed the main chute riser, releasing the main chute from the SRC and preventing the main chute from dragging the SRC across the desert. The main parachute deployment provided an aluminized mylar target with an effective radar cross-section of 1 square meter (10.8 square feet) to enhance the performance of radar-based

tracking assets. In addition, the SRC provided an ultrahigh frequency (UHF) beacon as an aid for tracking and locating the SRC. The UHF beacon was activated upon main chute deployment, its antenna located in one of the three legs of the parachute bridle that attach the main chute to the SRC. The UHF beacon radio frequency (RF) output was 100 milliWatts, providing a signal for tracking from either the recovery helicopters or ground vehicles using UHF direction finding receivers. (Unfortunately, during the actual recovery, due to the geometry of the landing, the beacon signal was blocked by the SRC, resulting in spotty reception; see Appendix F).

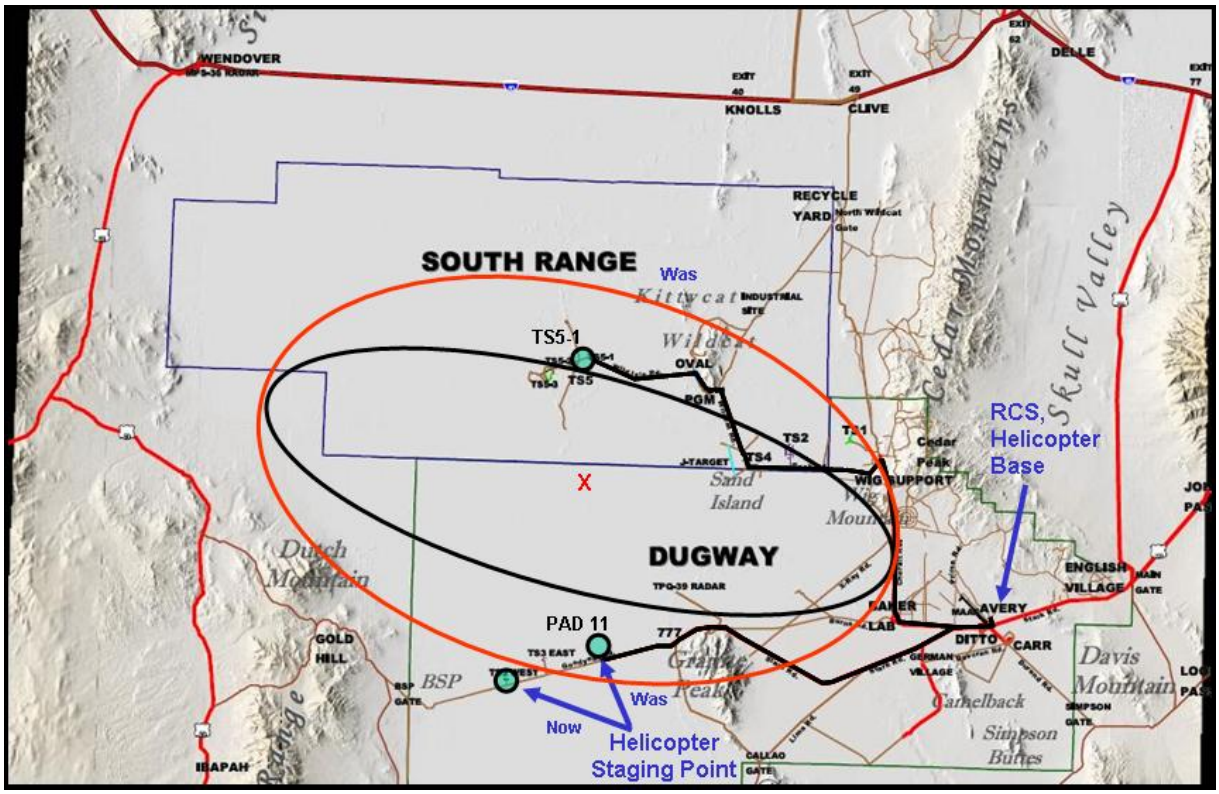



**Figure 10-2. Stardust SRC Recovery Ellipse at UTTR**

Although the requirement was to locate the SRC within 20 hours after landing, it was important to the science team to locate the SRC as quickly as possible since the potential for contamination increased with time. The aluminized mylar target and UHF beacon were the main tracking aids, but other tracking methods were also employed, including United States Strategic Command (USSTRATCOM), and UTTR infra-red (IR) tracking, to maximize the speed with which the SRC was located. USSTRATCOM initiated track of the spacecraft and SRC prior to SRC release. This tracking data was a valuable backup to primary tracking methods and was sent real-time to the project to improve the SRC trajectory confidence during the high altitude part of the descent. One of USSTRATCOM's assets (designated System X) was expected to track the SRC to the ground and pinpoint the landing site well within a square mile. Another tool used to update the anticipated landing location was high altitude weather data, collected in order to reduce the size of the recovery footprint by removing uncertainty in the atmospheric density and winds. Based on this data, the navigation team computed an updated nominal landing point and a correspondingly smaller recovery footprint. The weather data was also used to predict trajectories for the descending drogue chute with main chute bag attached.

The results of these trajectory analyses were provided to the Mission Control Center (MCC) at Hill Air Force Base (AFB), see Figure 1.6, to aid in acquiring the SRC during entry. Recovery personnel deployment, under the authority granted by the Recovery Commander located at UTTR, baselined using helicopters, but with a ground vehicle backup in the event of an anomaly, was based primarily on the data

received directly from range assets, which tracked the SRC from acquisition to landing, including C-band radar skin tracking enhanced by boresighted IR and visual capabilities. Once one asset acquired the SRC, the other radar and all optical/IR trackers were pointed to the same vector for acquisition.

Safety requirements levied by NASA, UTTR and LMSS were followed in locating, preparing, and transporting the SRC. The application of a clean, dry gaseous Nitrogen ($GN_2$) purge of the sample canister was required to ensure the sample canister interior remained pristine. Although the canister vent had a filter to protect against ingesting contamination, it was necessary to attach a $GN_2$ purge to limit water vapor saturation of the filter. Upon retrieval from the field, the SRC was transported to a portable clean room facility at Michael Army Air Field on Dugway Proving Grounds near Recovery Command (RCS in Figure 10-2). The sample canister was removed from the SRC and, along with all recovered flight hardware, was transported to JSC in Houston, Texas two days after recovery. At JSC, the canister was processed into a Stardust laboratory where the canister was opened and the aerogel sample grid handed over to anxiously waiting members of the PET.

## Sample Recovery Capsule Recovery Team

The recovery team was a multi-functional, multi-organizational group of scientists, engineers, technicians, pilots and safety experts. Based on the recommendations of the Genesis MIB, Stardust implemented a Recovery Command System (RCS) tailored after the Federal Emergency Management Agency's Incident Command System (FEMA ICS) to manage and coordinate all personnel, in particular since each element normally reported to their own home agencies and institutions. The blue elements of Figure 1-2, in Chapter 1, illustrate the components of the RCS. At the head of the RCS was the command group, basically project management, with sub-elements of planning, operations and logistics. The operations group not shown in Figure 1-2 had essentially the same make up as the Planning group, but with a different lead engineer who was focused on operational proceedings. This clarification was made within the Recovery Command System Plan [ref R7] developed early during the return preparations, and approved after test and training had been completed.

The RCS philosophy was to enable decisions to be made by recovery field personnel within the arena of approved operations procedures, nominal and contingency, with appropriate reporting of progress as the procedure was implemented. However, the Recovery Commander anticipated much more involvement in the event of an entry, descent, and landing anomaly. In addition, the Recovery Commander was the conduit to non-project ranking officials as required by the anomalous scenario. For example, a breakup and burnup scenario with debris landing outside of UTTR called for contacting and transferring command to the Lead Federal Agency Contingency Coordinator (LFACC) located at NASA Headquarters for coordination with other federal and state agencies in the hardware recovery process. These external processes are described in more detail in Chapter 9.

During operations, the Recovery Command Center was located in a building near the helicopter landing strip and the hanger that housed the portable clean room that was to be used for SRC processing. Voice and video communications within UTTR and Hill AFB were easily accommodated, including entry tracking and weather displays, communications with helicopters and on-scene recovery team members, and voice and video communications with personnel located back at JPL, LMSS, and USSTRATCOM. Unfortunately, during the actual return operations, the command center became crowded and congested, a lesson that is discussed further in Appendix F. However, the day's events were aided by implementing a premise of the FEMA ICS that called for the incident commander to be easily located and identified. The Stardust Recovery Commander accomplished this by wearing a flight suit of a different color than the suits worn by other recovery personnel, with the addition of a large Stardust logo on the back.

### *Field Personnel*

Helicopters were selected as the primary recovery vehicle as they would provide the quickest transport of personnel and recovered hardware between the landing location and the base of operations at Recovery Command. Ground vehicles provided backup capability to recover the SRC in the event the helicopters

could not fly due to a mechanical breakdown or, more likely, unacceptable flying conditions. The make-up and role of the SRC field recovery teams, subdivided by the transportation vehicle each was assigned to, is summarized in Table 10-1, and their functions are described briefly in Table 10-2. Though no vehicle is designated for the Breach Team, one of the vehicles would have gone back to home base in the event this anomaly presented itself.

Note that the Blackhawk column is crossed out in Table 10-1. The initial recovery plan was based on 2 commercial helicopters (Vertigo, Southcoast) and one Army National Guard Blackhawk. A contingency plan (use of a Long Ranger) had been established for the scenario where the Blackhawk was not available due to other military commitments. Three weeks before Earth return, the Blackhawk was called away and the recovery process was performed according to the contingency plan. In addition, military commitments had kept the Blackhawk and its flight crew from participating in test and training activities, which would have also resulted in implementation of the contingency plan (see Chapter 11 for more detail). These events affected the field personnel deployment strategy since the size of the field team was nominally 19 people with the Blackhawk helicopter. With the loss of the Backhawk, the field team was limited to 14 people. Furthermore, had one helicopter not been available on recovery day, the team would have been limited to 10 people, which was the same team size if the helicopters couldn't fly and the two ground vehicles had to be used. In retrospect, it would have been much more efficient to have planned for all helicopters being from the commercial partner. The coordination of flight activities would have been smoother and training more like the recovery mission.

**Table 10-1. Recovery Teams and Vehicle Assignments**

| Vertigo Helicopter Team | Southcoast Helicopter Team | ~~Blackhawk Helicopter Team~~ | Long Ranger Helicopter Team | Ground Team Vehicle 1 | Ground Team Vehicle 1 | Breached SRC Team |
|---|---|---|---|---|---|---|
| Helicopter Pilot A | Helicopter Pilot B | ~~Blackhawk Pilot A~~ | Bell Pilot | EOD A/Driver | EOD B/Driver | Science Co-I B |
| Co-Pilot/DFO A | Co-Pilot/DFO B | ~~Blackhawk Pilot B~~ | OSCAR 2 | OSCAR-1/EOD | OSCAR 2 | Curation Specialist B |
| OSCAR-1/EOD | QA/Safety Specialist | ~~Crew Chief A~~ | Recovery Team Field Lead | Recovery Team Field Lead | Physical Security Specialist | Recovery Specialist C |
| Safety/QA Specialist | Recovery Specialist B | ~~Crew Chief B~~ | Recovery Specialist A | Curation Specialist A | Science Co-I A | Recovery Specialist |
| | | ~~OSCAR 2~~ | Science Co-I A | Safety/QA Specialist | QA/Safety Specialist | Ordnance Safing Specialist |
| | | ~~Physical Security Specialist~~ | Curation Specialist A | Recovery Specialist A | Recovery Specialist B | |
| | | ~~Recovery Team Field Lead~~ | | | | |
| | | ~~Curation Specialist A~~ | | | | |
| | | ~~Science Co-I A~~ | | | | |
| | | ~~Recovery Specialist A~~ | | | | |

Minimum Team: Primary Helicopter Team + OSCAR Bell Long Ranger Helicopter Team (10 personnel)
Nominal Team: Primary & Secondary Helicopter Teams + OSCAR Blackhawk Helicopter Team (19 personnel)
Breached Team: Primary & Secondary Helicopter Teams + OSCAR Blackhawk Helicopter Team + Breached SRC Team (24 personnel)

The most significant contributor to the success of the recovery operation was the composition, capability and cross training of the multi-organization field recovery team. Due to the desire to minimize the number of people in the field along with the limited capacity of transport vehicles, the recovery team was comprised of very capable people who were cross trained for numerous recovery procedure tasks. Seven core members of the recovery team provided detailed technical, safety, quality assurance, curation and science expertise along with the capability of backing up each other in the event of injury during the operation.

## Recovery Operation Details

The recovery timeline was a sequence of events comprised of locating the SRC, recovering it from the field, delivering it back to the clean room, and preparing it for shipment to JSC. The actual recovery operation followed the baseline plan very closely. As a result, the following sections describe the as-implemented recovery operations, which, given the hands-on nature of the sample return mission and the accompanying available photographic evidence, provides a better illustration compared to the general discussion of the previous chapters. Planning and preparation for off-nominal conditions, not implemented on Stardust, are discussed later in this chapter.

**Table 10-2. Recovery Team Functions**

| Position | Function and Responsibilities |
|---|---|
| Pilot | Safe helicopter operations, transport of personnel and SRC |
| Co-Pilot / DFO | Assistant to Pilot, visual search for SRC, searchlight operation. Assists with securing SRC inside helicopter. |
| OSCAR-1 / EOD | Survey of landing site for unexploded ordinance, authorization of additional helicopter landings and all recovery activity. Initial examination of landed SRC, definition of approach and departure routes, and keep-out zones. Primary communicator with RCS. |
| OSCAR-2 | Assistant to OSCAR-1. |
| Recovery Team Field Lead | Overall responsibility for implementing the recovery procedure, maintaining communications with RCS, and declaring whether recovery was nominal or off-nominal. Assistant to recovery specialists in lifting, double bagging and securing the SRC inside the transport vehicle. |
| Safety / QA Specialists | Implementation of procedure safety steps, including NSI state and battery breach. Cross-trained for QA tasks. |
| QA / Safety Specialist | Monitoring implementation of all QA requirements, including hardware or operational verifications and procedure compliance. Cross-trained for Safety tasks. |
| Recovery Specialist | Implementation of procedure retrieval steps, including double bagging, lifting and placing the SRC in handling fixture, and securing the SRC inside the transport vehicle. |
| Curation Specialist | Assistant to determining the state of the SRC. In the event of a breach, responsible for implementation of the corresponding off-nominal procedure steps. Also operated a still camera for safety, curation and media needs. |
| Science Co-Investigator | Assistant to determining the state of the SRC. Implemented soli and atmosphere sampling procedure steps. In the event of a breach, participation in the corresponding off-nominal procedure steps. Operated a video camera. |
| Driver / EOD | Safe ground vehicle operations, transport of personnel and SRC. Cross-trained in EOD tasks. |
| DFO = Director of Flight Operations, EOD = Explosive Ordnance Disposal, NSI = NASA Standard Initiator, OSCAR = On-Scene Commander, QA = Quality Assurance | |

### *Finding the Sample Return Capsule*

The search for the SRC began two hours prior to entry when the recovery crews were briefed on weather conditions (temperature and winds) and the latest prediction of the SRC's landing ellipse as provided by the flight operations team, which also led to confirmation of vehicle staging locations. At this time the Recovery Commander also confirmed authorization for the Recovery Team Field Lead to implement the approved recovery procedure, operating autonomously from this point until delivery of the SRC and its contents to the JSC clean room as long as all activities were as defined in the procedure. After the briefing the recovery team gathered their field equipment, donned their highly visible, cold weather gear (Figures 10-4 and 10-5), and were transported to the helicopter hanger. Upon arrival at the hangar, a helicopter safety refresher briefing took place and recovery gear was stowed in the helicopters.

The three recovery helicopters, Vertigo, Southcoast, and Classic (the replacement for the Blackhawk) took 5 minutes for run-up, and approximately 15 minutes each to fly sequentially to their staging location on the southern edge of the landing ellipse. They remained on the ground at the staging area until the SRC had landed (based on range tracking data) and were instructed by MCC to proceed to the landing coordinates. In addition to MCC directions, the Vertigo and Southcoast helicopters were each equipped with a UHF direction finder receiver and antenna to assist in locating the SRC, and, since recovery was occurring at night, both vehicles were equipped with a high intensity illumination system (Spectrolab SX-16 Nightsun). During the nighttime training exercises for SRC recovery (discussed later in this chapter), the recovery team experienced the difficulty of finding a small dark capsule on the dark background of the dry lakebed, even with the powerful lighting. Additional IR sensors were added to the helicopter's instrument suite to detect the heat signature of the SRC. Since heatshield temperature during atmospheric entry was predicted at 2700°C (4900°F, albeit at the nose), the SRC was expected to stay hotter than the background desert temperature. As it turns out, during the actual landing, the SRC had cooled and the differential heat signature was minimal.

Vertigo (with OSCAR onboard) left the staging area first, headed towards the landing point identified by MCC, and performed on-site reconnaissance for the landed SRC. When the SRC was located, Vertigo

landed, following OSCAR's direction, and both OSCAR and the safety specialist exited the helicopter with their recovery equipment, moved to a safe position away from the helicopter, and Vertigo ascended to provide overhead lighting of the recovery area. In the mean time, Classic was authorized to proceed to the recovery location, with Southcoast following 9.5 kilometers (5 nautical miles) behind. OSCAR completed the area survey for unexploded ordnance, established a safe approach and exit route to the SRC and defined landing locations for the Classic and Southcoast helicopters, marking each location with blue and red beacon lights, respectively. Upon arrival, the Classic and Southcoast helicopters were authorized to approach their respective landing sites and land.

In addition to conducting recovery operations with proper consideration for human safety, one of the primary goals of the landing site operation was to preserve the condition of the interior of the science canister and cleanliness and physical integrity of the sample canister (Figure 10-3). To that end, helicopters and ground vehicle plans were designed to ensure approach to the SRC from the crosswind direction, thus avoiding potential contamination of the SRC and, in the event of a breached SRC, disturbance of any loose aerogel. In addition, helicopter standoff distance and altitude constraints for approach were a function of environmental conditions and defined in the recovery procedure.

***Recovering the Sample Return Capsule from the Field***

While the recovery team was in the field, continuous radio communications were maintained with the RCS, giving periodic status updates. Upon completion of the explosive ordnance disposal (EOD) assessment, the safety specialist was authorized to approach the SRC and evaluate its condition, following procedures for identifying and handling any unsafe conditions. This approach and assessment was conducted wearing a half mask respirator for protection against any potential harmful gasses.

**Figure 10-3. Stardust SRC Landed at UTTR**

Specific safety evaluations included verification of safe batteries with direct-read sulfur dioxide and acetonitrile detectors, verification of dissipated heatshield gasses with a hydrogen cyanide analyzer, verification of expended main parachute cutter by visual inspection, maintenance of a safe physical distance (centimeters) from the active UHF antenna, and avoidance of non-protected physical contact with the SRC surface.

After verifying a nominal SRC condition, two half-liter gas samples were taken from near the heatshield and from the SRC's backshell vents. Tape was placed over each vent in the backshell to protect recovery personnel from the possibility of in-transit rupture of the internal battery. Soil samples (and water samples, if present) at the touchdown point, along the roll path and final resting site were collected for contamination control purposes. The SRC was expected to be warm (the heatshield temperature could have been as high as 100°C or 212°F), so SRC handlers were required to use protective gloves. However, when the temperature measurements of the SRC exterior were taken at multiple points and recorded, it was revealed that the SRC had cooled to ambient levels. Photographs of the SRC were taken prior to moving the SRC from its landed condition.

Three people lifted the SRC by the heatshield perimeter (Figure 10-4), and, after verifying no significant mud was attached to the exterior surfaces, the SRC was double bagged and lowered onto a handling fixture. A sulfur dioxide monitor was set to audio alarm and placed between the two bags prior to sealing the outer seams with tape. The SRC was then ready to be placed into the Vertigo helicopter (Figure 10-5) for the flight back to the helicopter hangar.

The Vertigo helicopter carrying the SRC and safety specialist was dispatched from the landing site as soon as possible, while other members of the recovery team and vehicles remained in the field to complete environmental sampling and photo documentation. Upon returning to the helicopter hangar, the SRC was transferred from the helicopter to a pickup truck, secured and transported to the clean room building, where technicians were waiting to start the disassembly process. After offloading the SRC from the truck, the protective bags were opened, the tape placed over each backshell vent was removed and gas readings taken to verify the integrity of the battery. When verified as safe, the SRC was taken out of the double bags, placed on another handling fixture, and staged outside the entrance to the cleanroom.

**Figure 10-4. Three Person Lift and Carry of the SRC**

**Figure 10-5. SRC Double Bagged and Ready to Load on Helicopter**

***Disassembling the Sample Return Capsule and Preparing it for Shipment***

The science canister was separated from the backshell and heatshield of the SRC in the clean room at UTTR. However, the canister itself, which incorporated the avionics deck, remained sealed until delivery to a Stardust curation laboratory at JSC. LMSS was responsible for the disassembly of the SRC and removal of the sample canister; JSC curation and the science team supported the documentation of the process and inventory of recovered hardware.

Personnel were required to wear cleanroom smocks, shoe covers, hair/beard covers and cleanroom gloves until all components were packaged in clean containers. Access control limited the number of personnel in the clean SRC disassembly area to minimize the risk of contamination. Each piece of hardware removed from the interior of the SRC was handled with visibly clean tools (i.e. clean at 30.5 centimeters, 12 inches to the unaided eye) and was placed into a clean container or bag (visibly clean for metals and rigid plastics or equivalent for commercially cleaned bags). Precautions were taken to preserve the interior and exterior surfaces of the heatshield and backshell, and the surface of the science canister and avionics deck. During disassembly, personnel were cognizant of any pieces of the SRC bearing micrometeorite impacts or features of interest and flagged them for additional detailed analysis.

After the SRC's vents were verified to be clear of any obstruction (e.g. hardened mud), technicians drilled out the super lightweight ablator from the backshell, exposing and removing twelve backshell bolts, allowing separation of the backshell from the heatshield (Figure 10-6). After obtaining sample of the purge gas, a purge line was inserted through a septum into the sample canister with the purpose of preventing contaminants from entering the canister, and reducing the SRC internal humidity and temperature by using the clean, dry gaseous nitrogen. A purge log was initiated and maintained by the quality assurance representative to record purge times, cylinder identification and certification.

The SRC batteries and avionics, and six screws holding sample canister to heatshield brackets were then removed and the sample canister was extracted from the SRC heatshield, moving thermal blankets as required. Contamination control bags were attached to the two halves of the sample canister and the purge system, using a special clean room approved tape, to reduce the potential for sample

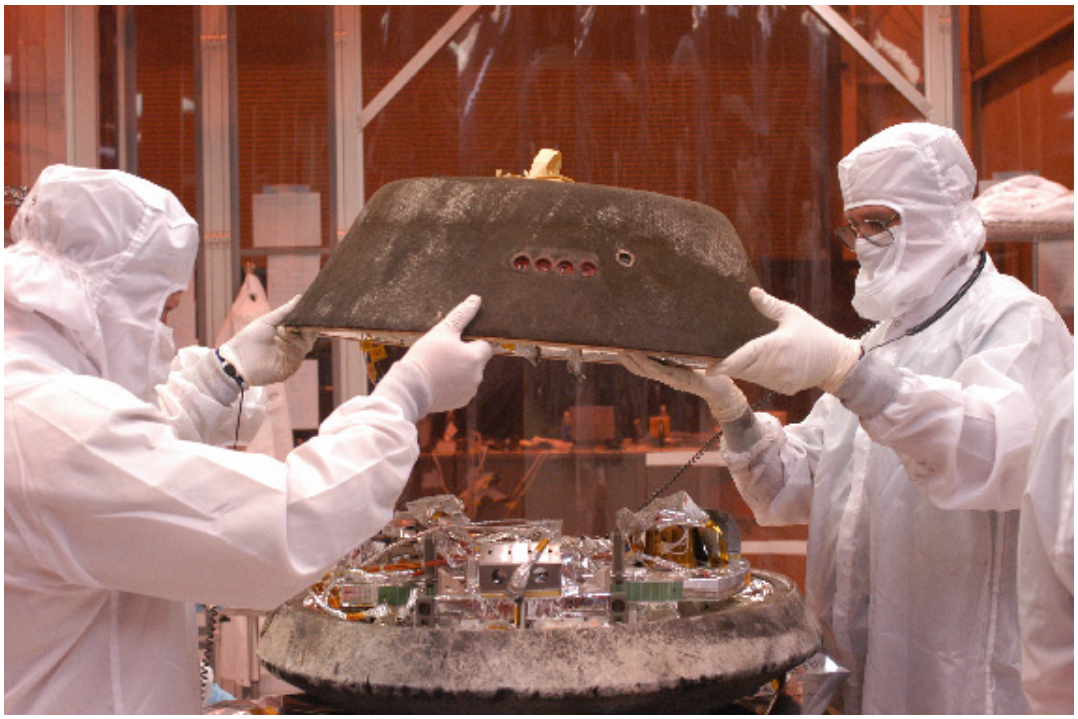


**Figure 10-6. SRC Backshell Being Separated from Heatshield**

contamination from the outside of the canister upon opening the canister at JSC. The sample canister with purge was placed in a handling and shipping container and environmental monitors were attached to track loads, temperatures, and purge flow rates during the trip from UTTR to JSC. The heatshield, backshell, and other SRC components were sealed in bags and placed in their respective handling and shipping containers for transport to JSC. All hardware remained in the clean room, under UTTR provided physical security, until it was ready to be transported to JSC. At this point, the recovery teams rested.

***Delivering the Sample Return Capsule to the Science Team at Johnson Space Center***

LMSS was also responsible for the safe and secure transportation of the sample canister, heatshield, and backshell from UTTR to JSC, including compliance with all Department of Transportation regulations. The hardware was transported from the clean room to an awaiting aircraft, a C-130, with UTTR security personnel providing physical security. The recovery hardware was flown directly from UTTR to Ellington Field, Texas where a JSC-provided ground transportation team and security personnel met it and affected the transfer to JSC proper, through the Space Exposed Hardware (SEH) laboratory, into a laboratory designed specifically for use by Stardust.

The sample canister's shipping container was opened, the purge disconnected and the sample canister was transferred into the SEH lab, where personnel removed the exterior bag, cleaned the exterior surface of the inner bag, re-wrapped the hardware in a new cleanroom bag (Figure 10-7), and secured the hardware to a cart for transfer to the Stardust curation laboratory. The canister exterior and all activities were photo-documented by a JSC Stardust team member.

Once the canister was transferred to the Stardust laboratory changing room, JSC and LMSS technicians put on clean room attire and then moved the canister and handling fixture inside the clean room. Photographs were taken before and after processing to document the condition of the canister. The canister was then unwrapped, unlatched, and opened, exposing the sample grid (Figure 10-8). Photographs were taken throughout the processing to document the condition of the sample canister and sample grid (Figures 10-9 and 10-10). The grid (with comet samples) was then transferred to the Science team, concluding the recovery activity.

**Figure 10-7. Rewrapping Sample Canister in SEH Laboratory at JSC**

**Figure 10-8. Sample Grid Ready for Handover to Stardust Science Team**

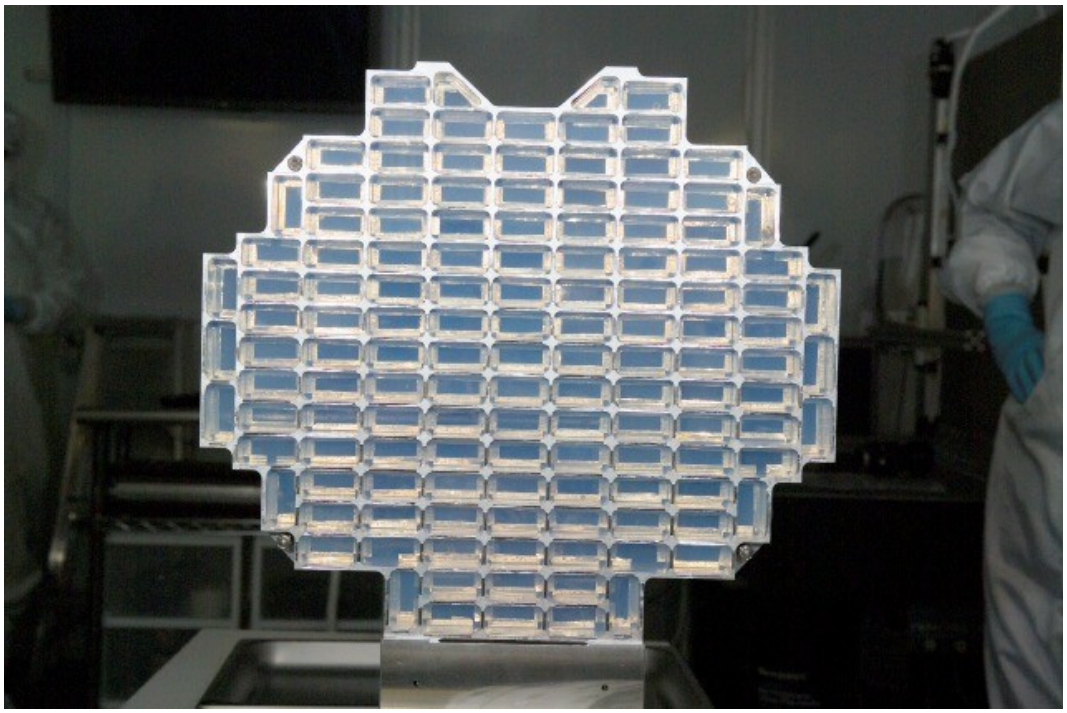


**Figure 10-9. Stardust Sample Grid Removed from Sample Canister**

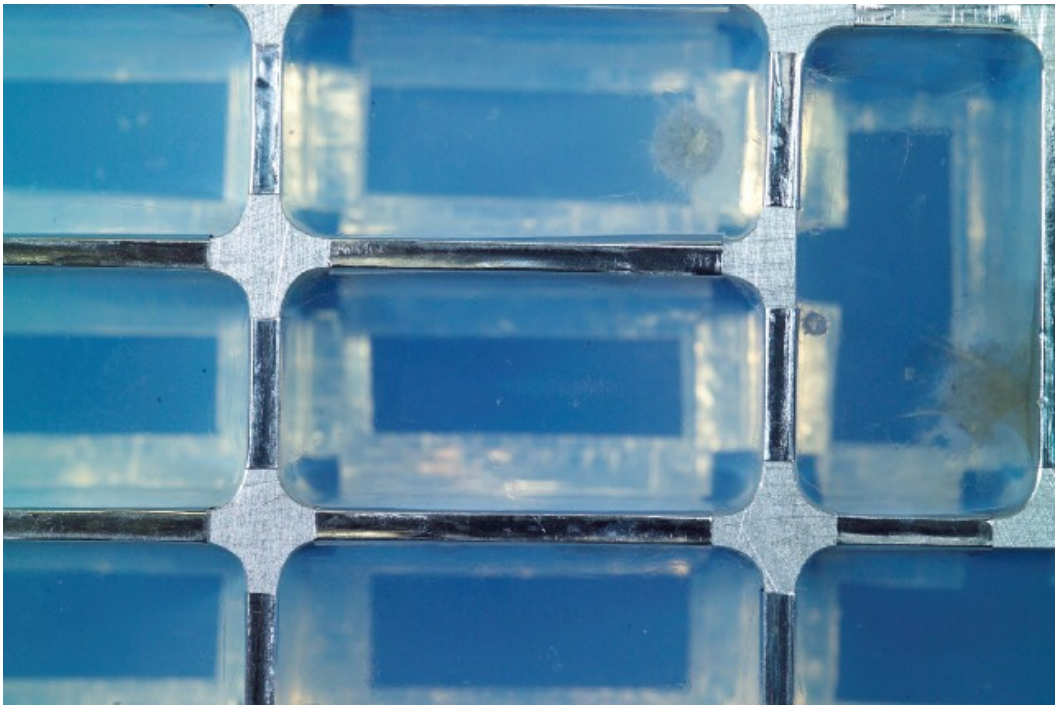


**Figure 10-10. Close-up View of Sample Grid with Cometary Particles**

## Off-Nominal Event Preparation

The Stardust recovery operations team planned, had equipment for, and were fully trained for all reasonable off-nominal SRC recovery scenarios. In fact, the majority of the training exercises focused on responses to off-nominal recovery scenarios. These scenarios were of two general types: those resulting from the SRC landing outside of the approved UTTR landing region, which were described in Chapter 9, and those that presented themselves within the approved landing region. In the former, recovery control was transferred to the LFACC, as described earlier. For the latter, the corresponding planned responses, and their reason for being selected are summarized in the following paragraphs.

### *Utah Test and Training Range Tracking Assets Not Available*

If the UTTR tracking assets (both radars, both IR cameras on the radars, all visual cameras (Cine-Ts) and the direction finding equipment) failed to track the descent of the SRC, a grid search process would have been implemented. Using the best trajectory data available from navigation and EDL propagation through the atmosphere, a most likely point of impact would have been identified and communicated to the recovery team. Radial search grids would have been defined and each helicopter recovery team would have been assigned a specific grid. Once the SRC had been located, both search teams would be called in to assist in the recovery operations.

The size of the search area would have been a function of when tracking data was lost. The more tracking data collected, the smaller the search area would have been. If no tracking data was generated, the search area would have been the entire a-priori 3-sigma footprint, starting at the projected SRC landing point generated by the navigation team, and progressing outward. If USSTRATCOM had tracked the SRC's reentry, but UTTR could not establish radar and UHF tracking, the expected 3-sigma search area would have decreased to less than 3.5 square kilometers (1 square nautical mile) with an aim point based upon USSTRATCOM's "System X" tracking data. (Unfortunately, USSTRATCOM's "System X" became unavailable to Stardust for actual recovery operation, see Appendix F for more detail).

### *Poor Weather*

If local weather conditions prevented the use of helicopters, ground tracked vehicles would have been used for locating and retrieving the SRC. Upon weather forecast indication of a reasonable probability of grounded helicopters, two ground vehicles outfitted with rubber track conversion systems (MATTRACKS, Figure 10-11) would have been staged outside the predicted landing footprint prior to landing. After the helicopters were actually grounded, teams would have removed the UHF direction finder (DF) receiver from the helicopters and would have loaded it, along with their other gear, into wheeled vehicles for transfer to the staging point (once cleared for movement onto the range), where the equipment would have then been loaded into the tracked vehicles.

After the SRC had landed, recovery coordinates would be communicated via radio to the ground vehicles that would then proceed to the coordinates while monitoring the SRC UHF beacon frequency. A search pattern radiating out from the predicted point of impact would have been implemented if the target coordinates were reached and the SRC was not visible. Once the SRC had been located, it would have been handled in accordance with the recovery procedures, placed into one of the vehicles and transported to a rendezvous point (nearest road) where the SRC would have been transferred into a wheeled truck, and transported back to the clean room hanger.

### *Breached Sample Return Capsule*

In the event of an off-nominal landing due to parachute failure or other condition, the SRC and sample canister could have breached upon landing and aerogel could have fallen out of the canister. The additional presence of winds could have also dispersed the aerogel downwind. The presence of water was detrimental due to aerogel's propensity for absorption upon contact. It was vital that any aerogel that had exited the SRC be collected as soon as safely possible to preserve the integrity of the collected

**Figure 10-11. Ground Vehicles with MATTRACKS Conversion Systems Installed**

samples. In addition, if the SRC had bounced, rolled, or been dragged from its original impact location, the aerogel could be dispersed over a 'fan' of downwind locations.

In the event of a breached SRC without a sample canister breach, three members of the recovery team would have lifted the SRC from the landing site and placed it onto a waterproof, heat resistant tarp. Excessive debris would have been removed from the exterior of the SRC, and the SRC would have been more closely inspected to confirm the lack of a sample canister breach. If no breaches of the sample canister were detected, the SRC would have been wrapped with a large piece of clean amerstat (a conductive plastic designed to prevent electrostatic charge build up), isolating the SRC interior from further potential contamination and the recovery would have followed the nominal plan for returning the SRC to clean room hangar. In the event of a breached SRC with a sample canister breach but no aerogel loss, the team would have followed this same procedure, but with additional care to not cause loss of aerogel.

For a breached SRC with sample canister breach and aerogel loss, the above procedures would have been used again for the SRC and sample canister hardware, but the remaining recovery team personnel would have collected aerogel pieces from the ground as soon as the safety specialist had ascertained that conditions were safe (Figure 10-12). All team members were equipped with an aerogel retrieval kit that contained pre-labeled sample collection containers, aerogel collection tools and a flashlight. Field team members not recovering aerogel would have obtained relevant environmental reference samples. Backup personnel and equipment (breached recovery team) would have been requested if necessary. These personnel would have been transported to the scene by helicopter or ground transport vehicle. Spotlights on the helicopters or ground vehicles would have been used to illuminate the ground surrounding the landing site.

Sample trays and packaged dry aerogel specimens would have been prepared for transport to JSC under the direction of the curation team. If the sample trays still contained aerogel, the nitrogen purge would have been established on the tray container. Transportation of the samples to JSC would not take place until all science and curation pre-ship processing was completed, regardless of how long it took.

**Figure 10-12. Recovery team rehearsing loose aerogel location and collection at UTTR**

***Extreme Mud or Standing Water***

Depending on ground conditions, it was possible that the SRC could land in mud or water. If the SRC landed in shallow water and upon initial examination it was established that neither its vents nor the heatshield-backshell seam had been exposed to water, the recovery would have been treated as a nominal landing with additional care being taken to ensure that water was not introduced to the SRC during operations.

If it appeared that the SRC had ingested any water, the SRC was to be lifted, and rotated, establishing a drain path at the backshell-to-heatshield seal joint, with the additional aid of a wedge tapped through the joint. All water drained from the SRC would have been collected, measured, and stored for subsequent analysis, as it could have contained aerogel or been a source of contamination. Once the flow of water out of the SRC had diminished to a slow drip or stopped, the SRC would be double bagged and placed on edge in the handling fixture and transported to the clean room hangar to be processed as quickly as possible. The field tarp was also to be rolled up, thus capturing any loose debris, placed in a duffle bag, and returned along with other environmental samples: soil (or mud) samples, and, in this case, water samples from any standing pools located at the site. Small containers and siphons were provided in off-nominal kits for this purpose.

Processing of the SRC in the clean room would have followed the nominal process until the sample canister was removed from the heatshield. At that point the canister filter would have been examined for moisture, and if present, the sample canister was to be manually opened and the aerogel processed according to the curation team procedures. All wet aerogel cells would have been removed and, each cell or fragment, placed in a dedicated labeled container and documented. If dry aerogel cells or fragments were free, each piece would also be placed in a dedicated labeled container and documented. As many dry cells as possible would have been preserved in their original tray positions, under purge as appropriate. Sample trays, packaged dry aerogel, and packaged wet aerogel specimens would have been prepared for transport to JSC under the direction of the curation team.

## Personnel Safety

Maintaining personnel and SRC safety during recovery training and operations was the highest priority recovery requirement. The Stardust Recovery Hazard Analysis [ref R8] was the source for recovery safety requirements. The hazards analyzed and documented therein are summarized in Table 10-3 and discussed in brief in the following sections. In addition to protective gear for various hazards, most critical to personal safety was the ability to see and communicate.

***Inclement Weather***

Personnel were prepared for cold weather conditions to prevent injury such as frostbite and hypothermia and to prevent SRC recovery inefficiencies due to physiologic response, e.g., loss of hand dexterity,

**Table 10-3. Hazard Matrix**

| Hazard | Phase / Configuration | Consequence / Likelihood |
|---|---|---|
| 1. Inclement weather | Field operations | Significant / Low |
| 2. Manual lifting | Field operations | Significant / Low |
| 3. Rough / hot surfaces | Field operations | Moderate / Low |
| 4.1 Inadvertent ordnance initiation, nominal landing | Recovery through ordnance disposition | Significant / Low |
| 4.2 Inadvertent ordnance initiation, off-nominal landing | Recovery through ordnance disposition | Significant / Moderate |
| 5.1 Helicopter physical hazards: Personnel clearance from rotors | Field operations | Catastrophic / Low |
| 5.2 Helicopter physical hazards: Ground article interference with rotors | Field operations | Catastrophic / Low |
| 5.3 Helicopter physical hazards: Drogue / sabot interference with rotors | Field operations | Catastrophic / Negligible |
| 5.4 Helicopter physical hazards: Excess sound | Field operations | Low / High |
| 6.1 Ablative burn products toxicity | Field operations and high-bay operations | Negligible / Negligible |
| 6.2 Battery vented products toxicity | Field operations and high-bay operations | Significant / Low |
| 6.3 Respirable aerogel | Field operations and high-bay operations, failed drogue or parachute deployment | Significant / Negligible |
| 7. Ablative inhalation exposure from backshell drilling operation to find fastener heads | High-bay operations | Significant / Negligible |
| 8. Skin irritation due to contact with ablative burn products during SRC handling | Field operations and high-bay operations | Moderate / Negligible |
| 9. SRC damage from mishandling | Field operations and recovery | Low / Moderate |
| 10. Asphyxiation from purge gas | Clean room operations/ Shipment to JSC | Catastrophic / Negligible |
| 11. Facility-related electrical exposure causing shock hazard | High-bay operations | Catastrophic / Negligible |
| 12. RF energy exposure | Field operations | Negligible / High |
| 13. Slips, trips and falls; body impact | Field operations and high-bay operations | Moderate / Low |
| 14. Skin puncture, abrasion | Field operations and high-bay operations | Moderate / Low |

mental focus, and shivering. Adverse weather could also affect the UTTR desert surface resulting in muddy or standing water conditions. Based on historical weather data, personal clothing was selected to accommodate an average minimum temperature of -6°C (21°F), average maximum sustained winds up to 13.3 kilometers per hour (8.3 miles per hour), and wet ground conditions. Except under the most abbreviated period of fieldwork, the weather could be expected to change from the initial conditions during recovery operations. Layered clothing was worn to accommodate a temperature range from -34°C (-30°F) to 4°C (40°F) and a wind speed up to 32 kilometers per hour (20 miles per hour). In addition to the ground vehicles and helicopters, shelter against the elements at the landing site was available to protect the SRC and facilitate SRC recovery in the event of an off-nominal landing.

### *Manual Lifting*

The SRC was handled manually during all recovery operations, but with the aid of a special handling fixture. Without the parachute, the SRC weighed approximately 43 kilograms (95 pounds) and required 3 people to lift and 2 people to carry and stow into and out of the handling fixture. To prevent differential lift strain, a “one, two, three, lift…” command was employed for all lifts.

### *Rough/ Hot Surfaces*

After atmospheric entry, it was anticipated that the burned thermal protection system on the exterior of the SRC would be coarse and charred. Personnel handling the SRC wore gloves and long sleeves to protect hands from abrasion. In fact, gloves were worn throughout the recovery process for additional weather protection and to protect the flight hardware.

### *Inadvertent Ordnance Ignition*

An inadvertent ordnance ignition hazard existed if there were ordnance devices that had not fired during EDL. Two ordnance devices could remain unfired even in a nominal landing: a drogue parachute deployment mortar NASA standard initiator (NSI) and the drogue parachute release cable cutter. The drogue parachute release cable cutter was a hand-safe device that posed minimal hazard if inadvertently fired; it was designed to function without creating debris. However, there was no practical field access to evaluate the drogue mortar NSI, and an inadvertent firing could eject debris out the drogue mortar tube. As a result, one NSI was assumed unfired during initial approach to a nominally landed SRC and eye protection, such as safety glasses, was required for personnel within 3 meters (10 feet) of the drogue mortar output. A diffuse plug was placed in the drogue mortar tube, after which safety glasses were no longer required. The plug was temporarily secured to the SRC parachute canister with tape to prevent the plug being inadvertently removed during handling.

Off-nominal entry would add to the ordnance hazards through failure in drogue deployment, main parachute deployment, and main parachute jettison upon landing. If the drogue failed to deploy, it would have been assumed that the ordnance was live and could fire at any time resulting in drogue deployment. The drogue assembly length was approximately 10 meters (34 feet), so a keep out cone angle zone approximately 12 meters (40 feet) in the direction of deployment would have been maintained until either the ordnance was disconnected from the avionics or the batteries were disconnected from the avionics. Personnel approaching within 12 meters (40 feet) to perform ordnance or battery disconnection would wear safety glasses.

### *Helicopter Physical Hazards*

Physical hazards associated with helicopter rotors were present during helicopter operations in the form of danger to personnel and interference from ground equipment. Prior to each operation, the flight crew briefed personnel of the hazards, including adequate clearance from both the main and tail rotors and the proper route to approach and egress from the helicopters. Other personnel were to remain clear of helicopters with powered rotors. Hazards from ground equipment being drawn into a powered rotor, in particular the SRC's parachute and personnel clothing, were addressed by securing those items when near the helicopters.

### *Gas Toxicity*

Two toxic gas sources on the SRC led to the requirement for the first person approaching the SRC to wear a half mask respirator and to again don the respirator while verifying that toxic gasses were not present prior to opening the SRC. The first source was the phenolic impregnated carbon ablator (PICA) heatshield, expected to produce benzene and carbon monoxide during atmospheric re-entry with subsequent collection in the SRC through the backshell vents. The second source was the SRC battery, whose electrolyte was a combination of sulfur dioxide, acetonitrile, and lithium bromide and would have produced sulfur dioxide and acetonitrile as a result of cell venting from an electrical short or excessive temperature.

## Recovery Operations Training

The purpose of the recovery team training program was to educate people so they could safely carry out all required SRC recovery tasks. Most training took the form of participation in formal training exercises

and operational readiness tests (ORTs). Cross training was implemented to the maximum extent possible to enable operational flexibility in the field.

The definition "trained" was established in accordance with project training requirements. Individual training and certification records were created and maintained for each team member. Training activities included individual training, orientation seminars, intra-team training, and inter-team training (rehearsals, test exercises, ORTs, and final wall-clock dress rehearsal). When possible, personnel training was accomplished concurrently with other activities. In addition, The SRC recovery operation took place at 3 am in mid January with a full moon. While training exercises were held at similar time and moon cycles, the ability to have cold and/or wet conditions was hit or miss. Fortunately, the Stardust recovery training did encompass these conditions without having to relocate the team in search of environmental challenges. Future missions may not be so fortunate and should plan accordingly.

To keep the training costs reasonable and enable rapid repeating of exercises, numerous training aids were used. The majority of the training exercises did not require an operational SRC, just a replica of its size, mass and center of gravity. The Stardust team fabricated such an article that enabled multiple iterations of each exercise to occur without having to reconfigure the SRC, avoided the risk of damaging the SRC structural thermal model with water and mud, yet maintained full fidelity for locating and handling the SRC. The SRC UHF beacon was configured as a stand-alone item with a commercial battery. This enabled SRC locating exercises to take place in parallel with SRC recovery exercises. The significance of these articles in keeping costs low and maintaining schedules cannot be overstated. In addition, one of the important factors in the recovery operations planning and implementation was the early definition and design of the interfaces between the SRC, handling fixtures, helicopters, ground vehicles, retention straps, etc. Once established and verified, they were not changed which prevented any late modifications to recovery equipment and procedures.

***The Training Plan***

Ten SRC non-drop recovery tests were conducted before a final wall-clock drop test exercise. During each test, the relevant portion of the recovery procedure was followed and redlined. A test debrief was held at the end of each test exercise and the recovery procedure updated to reflect all lessons learned. The training program started at JSC with a test of the procedure for sample canister receipt and processing into the Stardust laboratory. The recovery team procedure for opening the sample canister and extracting the aerogel grid was followed by the science team procedure for sample receipt, processing, and storage.

The first recovery operation field test was conducted in daylight without the helicopter and UHF DF equipment, and under the assumption that the drogue, main chute, and main chute cutter had operated correctly. This test exercise was repeated until no additional changes were made to the nominal recovery procedure for safety or technical reasons. The next daylight test exercise involved recovery under nominal landing conditions but assumed that water had been ingested into the SRC. The two tests were then repeated at night to evaluate the impacts of darkness on the safety and performance of the recovery procedure. The next series of tests simulated off-nominal landing scenarios such as the main chute still attached, unfired pyrotechnics, and breached SRC at night.

The final non-drop test prior to the use of the helicopters was an ORT scheduled for October 25, 2005 at UTTR. The SRC test article was placed at a location within the simulated landing error ellipse and with the UHF beacon active. The recovery team was provided a "tracked" landing point for SRC recovery. The recovery process then followed the ground team recovery procedure; no helicopter operations were involved. The test scenario included the RCS command structure and simulated interfaces with spacecraft flight operations, USSTRATCOM tracking, and Hill AFB tracking

After all aspects of the recovery procedure had been validated, the tests were repeated with the use of helicopters and UHF DF tracking, at Lake Elsinore, CA, to minimize test costs. The first helicopter test was in daylight to ensure recovery team safety. After the helicopter safety procedures were validated, the remaining testing was conducted at night - first with the nominal recovery scenario, followed by a

simulated breached SRC. The recovery test process then moved to UTTR for two ORT/ground recovery night tests with the full RCS command structure and simulated interfaces with the spacecraft operations team and tracking assets. The first test was a repeat of the October 25 ground recovery test, but at night in cold/adverse weather conditions. This was followed by a night test of the ground recovery of a breached SRC. Ground vehicles equipped with the rubber track conversion system were used during both of these test exercises.

A full drop test of the SRC was the final element of the Stardust recovery team training and certification plan. The test was conducted in conjunction with the spacecraft flight operations team wall clock ORT and integrated all STRATCOM, RCS and Hill AFB tracking functions. The test was conducted with close to a full moon to replicate the expected natural light conditions of the actual, January 15, recovery operation. The recovery portion of this integrated test started with the release the SRC test article from a helicopter at an altitude of approximately 3048 meters (10,000 feet) over UTTR with a modified parachute deploy sequence for the SRC (static line deployment of the drogue parachute). UTTR assets tracked the SRC and parachute and the recovery operations were conducted according to procedure. The results of the drop test were used to certify the readiness of the Stardust recovery operations team.

Integrated RCS training was accomplished in conjunction with three recovery test exercises and the drop test at UTTR. The recovery training exercises were initiated and monitored by the RCS from the Recovery Command. In addition to the training benefit, all test exercises that involved the recovery team accessing UTTR ground space or the release of the Test SRC from a helicopter included full RCS participation.

The recovery team test plan also included time periods allocated to recovery team rehearsals. These periods were devoted to conducting recovery activities without the requirement for a test procedure. The recovery team had the opportunity to practice key steps of the recovery operation in adverse conditions to ensure their proficiency.

The Stardust program management team had the option of increasing the recovery test and training program based upon the results of the plan identified above. There was also an opportunity for a second drop test if required, assuming the drop test article was functional. However, additional testing was not required due to the demonstrated performance of each recovery team member.

### *Independent Observers*

The majority of the recovery training exercises were witnessed by members of an Independent Review Team (IRT), formed to provide oversight and assessment of the readiness level of the Stardust recovery team. The IRT functions are discussed in more detail in Chapter 11. From a training perspective, the logistics involved with deploying the IRT prior to an exercise and ensuring their safety in the field was not trivial. It required vehicles, range safety, EOD escorts, and close communication and coordination with training personnel. In addition, having a multi-person review team staged ahead of time at the 'hidden' SRC location resulted in the recovery team finding it easy to spot the group of people and their vehicles rather than the small SRC.

### *Additional Certifications*

*Helicopter Pilots*

All helicopter pilots involved in the SRC recovery operation and preceding training events were certified by the Federal Aviation Administration (FAA) standards and physically able to execute their tasks. Evidence of each commercial pilot's current FAA approved certification, showing qualification for the aircraft to be flown, was provided to the RCS team prior to flight. In addition, all helicopter pilots were in possession of a 2nd class medical certificate, which was required for participation in the recovery operations and is a typical requirement when exercising the privileges of a commercial pilot.

*Helicopters*

An FAA Form 337 was required each time an aircraft was modified or altered with the installation or removal of special equipment such as night lighting equipment. (The FAA Form 337 is a conformity statement and approval for returning an aircraft to service after a major repair or alteration.) As such, a 337 form for each helicopter was filed prior to flights at UTTR, preceded by inspection by a qualified individual for the installation of equipment. For example, rear seats were removed from the Vertigo helicopter to accommodate the SRC. The passengers who rode in the rear seat area of the vehicle sat on removable cardboard fixtures that were designed to provide the same cushioning performance as a regulation seat in the event of a hard landing. The rear seat belts remained operational in this configuration. The seat modifications and helicopter operations plan were also subject to the review and approval of the NASA ARC Airworthiness Flight Safety and Operational Readiness Review Boards.

*Clean Room Operations*

All individuals with access inside the clean room were trained and certified prior to their initial entry into the certified clean room. Training activities included contamination control awareness, physical cleanliness requirements, proper entry and egress procedures, and equipment cleaning and handling. Only personnel who completed this training were permitted to enter and work in the contamination controlled areas.

## Summary

The flawless recovery of particles from Comet Wild 2 on the morning of January 15 was a direct result of the extensive and comprehensive planning and training described in this chapter. The hands-on, in-the-field nature of the recovery effort required proper balance between preservation of the samples and human safety. Chapter 11 contains additional information regarding compliance with agency and institutional standards for the latter, but said balance fell squarely on the shoulders of the recovery personnel. The recovery effort also required significant interaction between multiple agencies and organizations. The recovery command system was effective in organizing and managing both the planning and preparation process, as well as the actual implementation.

The preliminary science results coming from the analysis of the Stardust samples are exciting. In addition, storage of the SRC heatshield, backshell, and canister in JSC's SEH laboratory will enable scientists and engineers to examine this flight hardware to determine the environments to which the samples were exposed and evaluate engineering performance. The SRC is to be delivered to the Smithsonian National Air and Space Museam after completion of these activities.

# Chapter 11: Recovery Safety

As mentioned in Chapter 1 there was a cultural change within the NASA community regarding risk following the Columbia Accident Investigation Board report and the mishap of the Genesis sample return. The Genesis Mishap Investigation Board (MIB), in an early recommendation to the Stardust Project, stated the paramount importance of the safety of the ground recovery crew.

An Independent Review Team (IRT) was formed on the heels of the Recovery operations review six months prior to Earth return. This group focused on making sure potential hazards associated with human safety while handling the sample return capsule (SRC) in the field were mitigated and controlled. This group independently analyzed the worst-case contingencies (e.g. a breached SRC) and reviewed the procedures and training plan to obviate risks associated with the retrieval of the SRC.

## Independent Review Team

The recommendations from the Genesis MIB included a rigorous review of the consistency and adequacy of recovery contingency requirements and corresponding scenarios (see Table 1-1, Chapter 1). At the outset of the Earth return preparation process, the bulk of this review was planned to be completed primarily within the project, with the aid of an independent representative from institutional system safety who was added to the project's staff, and through the participation of independent review boards in the formal review process. However, six months before Earth return, as mentioned above, review board members planted the seed that led to the formation of a multiple member IRT to provide a more comprehensive and in-depth assessment.

The primary objective of the IRT was to ensure the safety of personnel, and flight hardware from the time of SRC landing through delivery to the JSC curation facility. Responsibilities included review of recovery operations procedures for both nominal and contingency scenarios and validation of the flow of requirements from the recovery command system plan [ref R8], Stardust recovery hazard analysis [ref R9], contamination control plan, Stardust recovery team training plan, helicopter flight operations plan [ref R3], and the helicopter flight operations safety plan [ref R2, R4] into the procedures. Another priority of the IRT was to identify hazard areas not included in these documents and propose appropriate responses and additions to procedures. Prior to launch, the project had completed an Environmental Assessment (EA, see Chapter 9) as part of the launch approval process. The IRT also reviewed this assessment to confirm that all potential hazards were being addressed. Additionally, any assumptions that were made in the approved EA were reviewed to confirm that these were still valid.

As a result of their review effort, the IRT was able to provide inputs to the aforementioned documents and procedures in the following areas: proper use of personal protective equipment (PPE), safe handling and transportation of the SRC, effective and timely communications, coordination, and decision-making processes in support of safe and successful operations, thoroughness of contingency planning, completeness of the procedures, and realism and effectiveness of training exercises. The IRT also participated in various external reviews such as the UTTR Safety Review Board (SRB), the project Critical Events Readiness Review, and the NASA Office of Safety and Mission Assurance Review.

The thorough review of all documents and procedures enabled the IRT to provide objective feedback. However, occasionally, the feedback process was contentious due to different perspectives on whether a particular activity was being conducted safely. In addition, the project found it challenging to accommodate the IRT given its late addition to the preparation process. The IRT was a new entity and there were times when it was necessary to review the purpose of

the IRT, which was to "audit" every document and procedure to make sure all the safety requirements were being met.

In addition to the document review, the IRT had on-site duties to observe test and training operations for verification that procedures were being correctly interpreted and followed. The ground recovery team had a very detailed training matrix, which included both nominal and off-nominal scenarios and ensured that all personnel (both primary and backup) were involved in the training program. The IRT was ultimately satisfied that all simulated exercises had been performed. Several end-to-end tests were conducted "on the clock" with the full team. Those tests included dropping the engineering model of the SRC, helicopter retrieval of the SRC, and delivery to the clean room. The IRT observed each test with special attention to the safety procedures. For example, if the test involved picking up the SRC for handling and/or turning it over (to simulate draining water as if it had landed in water), the IRT observed the addition of a person (from 2 to 3) to the lift team, as per procedure, to ensure safety.

The IRT was present during most of the training exercises and stepped in to enforce the project's training certification policies after a test in which the Blackhawk helicopter was unavailable to participate (see Chapters 9 and 10). During this final test, the ground recovery operations team and the flight team simulated the end-to-end Earth return and recovery at the same time of day as the actual event (3 am) with all of the assets that would be used during the actual day of recovery. The Blackhawk helicopter did not participate as had been planned. A replacement helicopter was used in its place. The IRT felt that, since the Blackhawk had not participated in the test, it should not participate in the actual recovery. This was based on previously approved training certification criteria that stated no pilot would be allowed to participate in the recovery operation without having successfully completed all required training.

The project applied for a waiver to use the Blackhawk due to the severe recovery personnel constraints associated with using a smaller helicopter for the recovery activity. However, the UTTR Chief of Range Safety declined the waiver stating: "*UTTR SRB states that aircrews that do not participate in the training activities will not be involved in the actual recovery operation. We are standing by this as a hard requirement. I have heard in many Stardust meetings that you will test what you fly and fly what you test. The same goes for training. No training, no participation.*"

The project complied with the policy and substituted a backup helicopter and crew that did not have the equivalent capabilities as the Blackhawk. However, the backup helicopter and crew had fulfilled the requirements for training and were able to participate in the actual recovery activities.

## Hazard Assessment and Analysis

In preparation for the Earth return, and in support of the risk assessment process, an end-to-end hazard assessment was developed by LMSS, the spacecraft contractor and recovery operations lead. The assessment had been independently reviewed by the JPL safety organization using the appropriate systems safety tools such as an independent preliminary hazard analysis, fault tree analysis, failure modes and effects analysis, sneak circuit analysis, energy conversion analysis, time sequencing analysis, etc. The IRT provided an additional independent review using information gathered from the recovery operations procedures.

Each identifiable hazard was screened for the appropriate control and mitigation approach. The prime areas for the analysis included re-entry ablation, aerogel dust exposure, training, facility and operational safety, contingency communication readiness, and the spacecraft disposal orbit. The summary matrix that was used to communicate the residual hazards is shown in Figure 11-1. Much like the mission operations assurance 5 x 5 risk matrix (Chapter 8), it was accompanied by a numbered hazard list and a detailed description of each hazard element.

| Safety Risk Matrix | | | CONSEQUENCE | | | | |
|---|---|---|---|---|---|---|---|
| | | | VERY LOW | LOW | MODERATE | SIGNIFICANT | CATASTROPHIC |
| | | PERSONNEL SAFETY | No injury/illness | No injury/illness | Injury/illness requiring a maximum of first aid. No admission to health care facility. No lost time | Injury/illness requiring attention of health care facility. Lost time. | Potential of permanent disability or death. Injury resulting in admission to health care facility. |
| | | HARDWARE SAFETY | No damage to flight or project critical hardware | Minimal damage to flight or project critical hardware | Damage to hardware. Damage repairable with minimal risk to project schedule or resources. Cost estimate=>$25,000 and < $250,000 | Damage repairable but definite impact to project schedule or resources. Cost estimate =>$250,000 and <$1 Million | Major damage, complete loss of hardware, or would require salvage or complete reconstruction. Cost estimate=$1 Million |
| | | ENVIRONMENTAL | No environmental impact | Clean-up with no impact on the environment or possible fine | Some damage to environment, but repairable, with no long term ecological impact. | Repairable damage to environment with potential for long term ecological impact. | Irreparable damage to the environment with potential for very long term ecological impact. |
| Likelihood | HIGH | Fair probability or likely | 12 | | | | |
| | SIGNIFICANT | Fair possibility | | | | | |
| | MODERATE | Definite increase in potential | | 9 | | | |
| | LOW | Possible or slight increase in potential | | | 3, 13, 14, 15 | 1, 2, 4.1, 4.2, 5.4, 6.2 | 4.0, 5.1, 5.2 |
| | VERY LOW | No determinable increase in potential | 6.1 | | 8 | 6.3, 7 | 5.3, 10, 11, 16 |

**Figure 11-1. Recovery Hazard Summary Matrix**

One example of hazard mitigation was the use of detectors during the initial approach to the SRC to analyze the air at the SRC, particularly near the vents, and determine whether potential toxic gases were present at a levels equal to or below the Occupational Health and Safety Administration health requirement. On Stardust, the following toxic gases were assessed on first approach and again upon arrival at the clean room hangar: sulfur dioxide, acetonitrile, hydrogen cyanide, and carbon monoxide. Chapter 10 described in detail the PPE required for the first responders approaching the SRC. This gear was included as part of the hazard analysis. In addition, the Material Safety Data Sheet was reviewed for other applicable controls. Other potential hazards that were considered were aerogel, respirable dust, ordnance recovery, radio frequency emissions, SRC handling, electrostatic discharge, ground support equipment, PPE for the cold weather, wind chill, etc., human factors, and transportation certification (including pilot's certification for medical clearance).

All operations or activities involving the SRC (critical hardware) that were considered hazardous were reviewed prior to Earth return. Safety surveys were conducted to assure compliance with regulatory requirements for personnel and facility safety.

## Safety and Mission Success Review

Previously known as the Safety and Mission Assurance Readiness Review (SMARR), the Safety and Mission Success Review (SMSR), is "*a NASA Headquarters Safety and Mission Assurance (SMA) and Office of Chief Engineer review that is held for the Chief SMA Officer and the Chief Engineer to independently assess the readiness to proceed with a high-risk program or project activities. The SMSR provides the basis for the Chief SMA Officer or a designee to knowledgeably and confidently sign the Certificate of Flight Readiness, or to issue a recommendation to the appropriate Mission Directorate Associate Administrator to proceed with the activity.*"

A SMARR was held prior to the Stardust sample return. The review focused on items related to residual risk to safety or mission success. In addition to the hazard assessments described in

this chapter, the review included the flight residual risks documented in the 5 x 5 matrix described in Chapter 8.

## Summary

The IRT was chartered to provide independent assessment to the JPL Environmental Health and Safety Program Office, the Stardust Technical Warrant Holder, the Stardust project office, independent review boards, and NASA Headquarters officials. IRT membership was composed of individuals with various backgrounds applicable to recovery operations from Aerospace Corporation, JPL, Ames Research Center, NASA Headquarters and Kennedy Space Center. A couple of the JPL members had also been involved with the Genesis recovery and as a result had recent experience with a sample return mission.

The success of the Stardust mission was due to the effort of the team that had been with the project from cradle to grave. The IRT was formed to have fresh independent eyes to review anything that might jeopardize the success of the mission. The success of the project and the team speaks for itself.

# Chapter 12: Summary

The preceding chapters of the sample return primer have provided future program managers and lead system engineers with a case study for architecting, planning, reviewing and implementing the final phase of a sample return mission. The programmatic and element-by-element guide described analyses, trade studies, operations plans, procedures, contingencies, interfaces and documentation, and a corresponding independent review process that achieved proper communication of residual risk to upper management and the required state of readiness in hardware, software and personnel.

Based on the experiences of lead engineers, the descriptions were naturally biased to the Stardust mission, as influenced by cultural changes resulting from the Columbia Accident Investigation and Genesis Mishap Investigation Boards and, as such, should be tailored to the specific future application. Given the anticipated time interval between Stardust and the next sample return, prudence dictates careful research into many of the NASA, institutional, and external support organization driving requirements, in particular in the areas of range safety, planetary protection, entry, descent, and landing, and ground recovery operations.

The primer's overview chapter provided a programmatic framework by describing the dual-phased independent review milestones. An eight-month risk identification, assessment, and mitigation review process was followed by a three-month (slightly overlapping) test and training, and readiness review process. The review processes were architected recognizing the interdependence of the mission and navigation baseline, characterization of event environments, conditions, and parameter sensitivities, certification of hardware and identification of mission contingencies, creation operations plans, procedures, and interfaces, and readiness certification through test and training.

The mission design and navigation chapter illustrated the steps that ensured the sample return capsule was delivered to the Earth's atmosphere with the proper conditions to achieve the desired landing location. The bulk of the flight operations activity, with exception of the capsule separation event itself, was driven by the needs of the terminal navigation effort. Recovery operations need be responsive to the predicted navigation error and credible contingencies. Key to the navigation effort was close and frequent communications with the attitude control spacecraft experts. Insufficient interaction between these teams during the initial Stardust preparation process led to the need to re-certify error modeling for the final trajectory correction maneuvers and attitude control behavior.

Conducted largely by the systems engineering personnel on Stardust, project compliance with range safety requirements (risk to population and property, primarily) is captured in the chapters describing the development of the Earth Targeting and Entry Safety Plan Volumes 1 and 2. Architected to be a one-two punch, Volume 1: Hazard Analysis constituted overall approval to conduct the final navigation targeting and sample capsule release events while Volume 2: Decision Criteria provided the processes for assessing event progress and enabling continued execution.

Perhaps more efficiently created during the development phase of a mission, the completion of the range safety analysis benefited from an instantaneous impact track that avoided major population centers and could rely on easily defendable spacecraft reliability parameters. However, the same hazard analysis was frequently questioned due to the relatively shallow set of real-world data that could provide verification and validation of break-up and burn-up analyses for vehicles similar in size to the sample return capsule. On the other hand, the decision criteria construct, built largely on the precedents established by the Genesis efforts, benefited tremendously from the scrutiny of the test and training program. Late, but fundamental, and perhaps still debatable, changes from quantitative criteria to qualitative criteria, and the addition of a criteria violation appeal process illustrated the value of a strong validation process. In

addition, the validation process revealed a quite significant criteria omission (entry flight path angle) illustrating the need during the development process to carefully and rigorously examine all parameter ranges and assumptions in the context of criteria independence.

The Genesis G-switch mishap accentuated the need for detailed examination and certification of the "as-built" sample return capsule and entry, descent, and landing systems described in their respective chapters. Nevertheless, conducting these activities in the absence of a preceding mishap was essential to properly convey and communicate the residual risks involved with the separation, and entry, descent, and landing operations. Both review processes were challenged by the need to recover detailed design specifications, requirements verifications, and vehicle close out records from prior to launch (7 years old), frequently encountering paper only products or inaccessible electronic files, thus illustrating the need for improvements in project library maintenance.

Certification of the correct operation of the Stardust G-switches was obtained by re-creating pre-launch verification and validation tests. These test were repeated several times, driven primarily by the need to simulate a flight like environment. Its performance thwarted by side-loading, initial G-switch tests did not provide sufficient vibration and produced results severely out of specification. Once the tests re-created the flight environment, the new tests validated the operation of the switch. Being its first flight, the entry, descent, and landing review provided the necessarily risk insight into the as-implemented thermal protection system on the return capsule. In particular, certification of the capsule's performance beyond the design entry flight path angle was essential to decision criteria process. The work maximized the landing area available to the delivery of the capsule to Earth and provided an understanding of the capability of the capsule beyond requirements.

To protect against review process expansion into an endless research project, a very real possibility and funding sink hole, the pending activities from these two processes were eventually binned and prioritized into three categories: those that could have direct effect on flight and recovery operations planning (example: entry flight path angle re-certification), those that would yield assessment information that would be of clear benefit during the return phases (example: non-grounded pyrotechnic firing circuit could brown out the capsule avionics and prevent the main parachute from deploying, thus leading to a hard landing), and those risks that would have absolutely no impact on any aspect of the remainder of the mission (example: what harness cables go through cable cutter 1 versus cable cutter 2). The last category was not pursued to completion.

The flight operations and flight mission assurance chapters contained the preparation activities conducted to plan, prepare, and characterize the spacecraft and mission operations executed in support of the final two weeks of the mission. In addition to implementing the terminal navigation plan, a key component of the spacecraft effort was the development of the sample return capsule release critical sequence. The sequence design robustly implemented the required capsule initialization, limited checkout, and pyrotechnic retention and release commanding, but was responsive to interactions (primarily by providing ground processing time) with the range safety decision process, mission success contingency identification and commanding process, and the on-board fault protection design.

The fault protection debate was interesting in that it revealed a philosophical dilemma that extended to the independent review teams. Was it better to leave the fault protection configured in a known state, with several tens of thousands of hours of flight experience while taking additional risk that a fault condition not essential to capsule separation could abort the separation event? Or was it better to change the fault strategy so that only those conditions essential to separation would trigger an abort, but taking the additional risk of insufficient validation and verification of the fault protection settings? The Stardust project biased their design toward the former. Overall verification and validation of the sequence and fault protection design was achieved with a thorough test program that made use of the high-fidelity spacecraft test

laboratory and included engineering development, logic branch, and spacecraft anomaly test components. Full subsystem test reviews and a rigorous test flag and associated configuration management plan ensured success of the test program.

Throughout the preparation processes, flight mission assurance focused its efforts on independent risk assessments of project plans. In addition, they provided an invaluable link to the project's development and flight history and to evolving institutional requirements through the review of flight incident, surprise, anomaly reports and major waivers, development single point failure lists, problem failure reports, unverified failures and waivers, and institutional project practices, design principles, and lessons learned from previous missions.

The Stardust sample return could not have been conducted without the participation of many external organizations. The required support architecture and infrastructure was described in the external interfaces chapter. The information contained therein provides not only how the flight and recovery teams interacted with these organizations during actual operations, but also described the requisite support agreement documentation and planning process. Varied in nature, the external support arena encompassed from non-NASA tracking assets to landing site support and curation expertise to contingency operations and risk communication with NASA HQ and federal agencies. Early and regular engagement with key personnel from each organization was key to the successful support provided for Stardust. However, the project also found it challenging to engage several of these organizations in end-to-end test and training as Stardust was only one part of their very busy portfolio.

The description of interactions with external agencies was followed nicely by the description of the recovery operations and recovery safety planning and preparation processes. The Genesis recovery mishap turned the bright floodlight of scrutiny on the preparation efforts and provided the impetus for a comprehensive and rigorous identification and preparation for all credible recovery contingencies. Adopting recommendations from the Genesis Mishap Investigation board, a Recovery Command System, modeled after Federal Emergency Management Agency practices, was adopted and all operational procedures, nominal and contingency, were placed in a single pre-approved document.

The brunt of the preparation effort was spent interacting with independent review teams and institutional safety representatives to ensure that all operations placed human safety first while achieving a proper balance with sample recovery success. This interaction culminated with the formation of an Independent Review Team who was chartered with detailed review of plans and procedures and in-the-field observation of selected training exercises. A great amount of effort was spent on ensuring that the test and training program was of sufficient breath and verisimilitude to the actual expected cold, night recovery operation. Independent review boards frequently challenged the project to re-create all possible contingency scenarios (breached capsule, breached grid, loose aerogel, wet aerogel) and weather conditions (rain, snow, fog, clouds, extreme cold).

The appendices that comprise the remainder of this document, the handbook, if you will, capture additional, mission specific, element-by-element lessons learned from Stardust. Several appendices capture observations beyond Stardust, offering suggestions applicable to the project life cycle and future vehicle design. Lastly, access to the project's library provides future planners and implementers with real-world examples of the review material and documentation produced during Stardust's final year of operations.

# Appendix A: Programmatic Lessons Learned

The Stardust management team successfully planned and managed the implementation of a rigorous and comprehensive risk and readiness review process despite being faced with radical changes to the project's standard operating culture resulting from the Genesis mishap and the Columbia accident investigation. In fact, second to developing the review and readiness plan, the biggest challenge was infusing the change in culture to the team, convincing them that the changes were necessary and for the benefit of the project. Overall, the preparation process was well managed and executed by the team, and lead to near perfect flight operations and flawless recovery operations. Nevertheless, during the course of the managing the effort, several Stardust specific lessons were learned, which are worthy of capture for future sample return opportunities.

## Communications with Upper Management

It is important to keep institutional management informed of both programmatic and technical status. Err on the side of passing along the information rather than omitting it. There were two examples of this benefit during the Stardust preparation phase. The first was the breaking of a funding logjam within hours of having notified key upper managers, after weeks of delay, in the support of the sample return capsule (SRC) and entry, descent, and landing (EDL) review efforts. The second is that, in addition to the technical expertise and guidance that can be provided by senior management, advance insights can be obtained as to the acceptability of project plans and responses to review action items. A corollary to this lesson is that senior management must tread carefully to insure the interaction with the project is in fact beneficial, a catalyst for the proper development and decision-making, as opposed to micro-management.

## Review Planning and Management

During the planning and execution of the review process, it was found to be extremely beneficial to standardize the planning, coordination, and execution of reviews. With a few exceptions, a single manager coordinated the Stardust reviews. While seemingly a trivial concept, the standardization eased the burden of conducting and organizing individual reviews and allowed the team to focus on the purpose and content of the review activity. Some execution standards (like hard copy handouts, not available at the EDL review) maximize the review board's ability to participate, while others (review board reports, not produced for the SRC system review) allow the project to have complete record keeping and appropriately manage responses.

## Review Board Construction

The constitution of a review board must be very carefully considered in the big picture of the worthiness of the review process. Proper coordination is necessary with the review board chair and senior management. For a review program or plan, maintaining continuity in the review board membership will allow the project team to focus on progress since the last review and not repeat the educational process. For Stardust, the review process benefited tremendously from participation, and, ultimately endorsement, of the Genesis Mishap Investigation Board (MIB) chairman, executive secretary, and other MIB team leads. In addition, document approval benefited from the participation of key signatories (institutional management, and the system technical warrant holder) in the review process.

## Review Requests for Action

Project responses to Requests For Actions (RFAs) could have been better managed and tracked more closely, in particular, disposition of the RFA with initiators. The latter was not done proactively on Stardust, rather it was assumed done by blanket electronic mail distribution. This created extra effort during the readiness review process to ensure that all open paper work was indeed closed per institutional requirements. Some of the confusion could have been averted by better management of those RFAs that were already captured by review board report findings (a very typical occurrence).

## Documentation Signatories

Despite attempts to settle on signatories for key project documentation early in the preparation process, the project continued to work this issue until just prior to return. The lesson is that this takes a long time, be aware of this and plan for it.

## Staffing Issues

Risk review processes can overwhelm compact end-of-mission plans, with remedial development tasks overlaying operational tests and readiness reviews, adding significantly to the burden of Earth entry operations preparation. In addition, long missions with operationally challenging spacecraft run the risk that the analysts with the appropriate experience will not necessarily be around for the final critical operations. It is advisable to document all procedures thoroughly and train new analysts in all new information derived to date.

For Stardust, calibration activities extended right up until the end of the mission, requiring extensive flight support, which had the potential to overwhelm the ground team when overlapping with the conclusion of the preparation period. For example, two calibration campaigns had been conducted during cruise operations, but a terminal attitude control trending plan was still required. At least two orbit determination analysts were dedicated (almost exclusively) to the trending problem for the last 6 months of the mission. They had additional support from attitude control analysts at LMSS and their work rippled through the rest of the flight team in so far as modifications to the primary flight plan and contingency planning.

# Appendix B: Earth Targeting and Entry Safety Plan Volume 1: Safety Analysis Lessons Learned

The description of the safety analysis preparation process and Stardust experiences contained in Chapter 3 mentioned the existence of several advantages and disadvantages worthy of note for future sample return missions. The most significant of these, comprising a disadvantage for Stardust, was the selection of materials from which the flight hardware was built. Discussed in more detail in Appendix G: Vehicle Design, selection of materials that completely breakup and burnup when entering the Earth's atmosphere would be a tremendous benefit to compliance with NASA and landing range safety requirements. The ability to provide this characteristic during future developments will, of course, be mission specific. At least one subsystem, the sample return capsule, must be designed, as robustly as possible, to survive to ground. Another lesson learned during the generation of the Earth Targeting and Entry Safety Plan safety analysis is captured below.

## The Stardust Instantaneous Impact Track

The importance of the incoming trajectory and corresponding instantaneous impact point (IIP) track cannot be overstated when attempting compliance with range safety requirements. It might event be argued that the importance of the IIP track may very well transcend the cold, hard analytical world that many engineers tend to live in (or at least prefer to live in).

Referring back to Figure 3-1, imagine, for instance, a hypothetical IIP track that approached UTTR not from the South-East, but from the North-East, cutting through the heart of the greater metropolitan area of Salt Lake City (less than 161 kilometers or 100 miles away). Visual inspection of the Stardust safety results suggests risk compliance would have required at least a couple more (if not more) orders of magnitude in discount factors (from spacecraft reliability, population sheltering, etc), effectively eliminating the bulk of conservatism that remained for Stardust. Not to be ignored, development and defense of these discount factors would have engendered expenditure of much more workforce.

But, where does the transcendence come into play? Not in the attempt to get external review board and document signatory buy-in with the technical arguments or analysis, which would have been challenging enough for Stardust, but more so within public perception and the development of federal agency contingency coordination and risk communication plans. Future missions would be wise to not open this Pandora's box and recognize the value of being able to state, with a fair amount of certitude, that there is (effectively) "no" chance of raining debris over downtown Salt Lake City compared to a series of statements that attempt to describe and characterize the low probabilities of producing debris and the chance that said debris would actually cause damage.

This is not to say the hypothetical North-East IIP track could not be successfully implemented. But it should be addressed early in the mission development phase - it is judged to be extremely challenging, and should be avoided if at all possible.

# Appendix C: Earth Targeting and Entry Safety Plan Volume 2: Decision Criteria Lessons Learned

The Stardust development and implementation of the Earth Targeting and Entry Safety Plan (ETESP) decision criteria provided the project with a robust and complete set of metrics via which to judge the return flight operations and ensure the operations were proceeding as planned. Indeed, implementation of the plan was relatively straight forward and with out incident with one exception: the presence of a sustained South wind that was near than the 3-sigma value modeled in Monte Carlo simulations of the atmospheric descent. This and other lessons learned during the Stardust implementation of the ETESP criteria are described below.

## The South Wind

The simulation of atmospheric conditions in support of the entry, descent, and landing (EDL) calculations that fed the decision criteria evaluation were predicated on the assumption that said conditions were typically too variable to warrant a late or real-time update prior to the final evaluation epoch. An updated weather prediction would have been required approximately 8 hours prior to the actual EDL in order to support the criteria process timeline. In all likelihood, the argument was, the weather would change between the time the atmospheric measurements were made and the actual entry. As such, it was deemed more appropriate to perform the criteria evaluation EDL runs with the historically based atmospheric models.

In parallel, however, the recovery team, for the purposes of adjusting recovery operations, put into place a process to release weather balloons, obtain updated atmospheric conditions, feed them to the EDL analysts, and track the movement of the landing ellipse predictions. The first of these updates was performed shortly after the final criteria EDL runs and was based on weather data from a balloon released 8 hours prior to atmospheric entry. The balloon data revealed a sustained wind profile out of the South that was 74 kilometers per hour (40 knots) at 4570 meters (15,000 feet) above sea level (ASL) to 18.5 kilometers per hour (10 knots) at UTTR ground level (1280 meters or 4200 feet ASL). Main parachute deployment was planned for just about 3048 meters (10,000 feet) ASL. The historical atmospheric model predicted no wind, on average, for this day and this time of year. A second update, based on weather data from a balloon released 2 hours prior to entry, revealed the wind was not only still present, but had grown a little in strength and was now 83 kilometers per hour (45 knots) at 4570 meters (15,000 feet) and 18.5-28 kilometers per hour (10-15 knots) at the surface. The landing location in the presence of these winds was predicted to be approximately 14 kilometers (7.5 nautical miles) to the North of the position predicted in support of the criteria evaluation (with no wind being modeled).

In the end, the atypical wind profile only pushed the landing location of the SRC about 7 kilometers (3.8 nautical miles) to the North of the pre-decision prediction (refer back to Figure 1.6) as a result of a break in the weather at the time of atmospheric entry. Unfortunately, balloon data was not taken at the time of entry to enable corroborating EDL modeling runs. The late break in the weather somewhat validated the original reasons for not including weather updates in the criteria calculations, and, on its own, the wind profile would not have affected overall mission compliance with the decision criteria. However, compounded with an anomalous scenario where some of the navigation criteria might have been borderline, the failure to acknowledge the effect of the wind could have led to approval for entry when indeed it should not have been.

For future sample return opportunities, consideration of actual atmospheric conditions should be revisited for formal integration into the ETESP decision process and the overall context of mission compliance.

## Yellow Divot and Probability of Creating Debris

Among the navigation decision criteria was one designed to protect against the possibility of there being a failure in the actual sample return capsule (SRC) release mechanisms that would lead to an unstable atmospheric entry, break up and burn up of the SRC, and raining of debris over populated areas to the South-East of UTTR. The region within the approved landing zone where the SRC could not be targeted to protect against the debris scenario was known as the Yellow Divot and was determined by establishing where the maximum value of population hazard for a collection of debris ellipses was greater than a discounted NASA population hazard requirement (see Figure C-1). There are two elements in the construction of the Yellow Divot concept that, while deemed appropriate for Stardust, would benefit from increased rigor in future developments.

The first element that could be improved is the discount that was applied to the NASA hazard requirement for the debris scenario. The project pursued rationale for discounting the NASA hazard requirement only to the extent necessary to produce a "tolerably small" Yellow Divot zone (as judged by project personnel, typically with a goal of having no intersection between the 3-sigma landing ellipse and the Yellow Divot zone). In general, the project accounted for the probability of occurrence in the hazard analysis, and, in many cases, the Stardust compliance was so robust that it could tolerate 100% occurrence. This was not the case for the debris scenario, where the analysis used 90% spacecraft reliability together with 60% probability of not producing debris, the latter attributed to the release mechanism (only 60% of the mechanism stroke was required to provide sufficient spin stabilization to the SRC to prevent tumbling). These discount values and arguments were pursued and utilized because they were easily adoptable, explainable, and accepted by review boards and approving authorities. A more rigorous and analytical approach in the determination of discount factors, like a probability risk assessment, or a quantitative fault tree approach, albeit requiring additional schedule and funding, may have allowed deletion of the Yellow Divot from the navigation criteria suite and increased the chances of success while retaining compliance with the NASA requirements.

The second element has to do with ensuring the decision criteria are being evaluated against the appropriate landing ellipse and understanding the sensitivity of the decision criteria to ellipse size and location. During test and training, the hazard analysts discovered that the ellipse being used for the debris hazard calculations was the ellipse for the intact SRC, not the debris field ellipse. The latter ellipse was about half the size of the intact SRC ellipse, and as a result the overall hazard probability increased to within striking range of the NASA requirement. In response, the project not only fixed the tools, and made the appropriate changes to the Yellow Divot, but also performed a location and ellipse size sensitivity study to understand the conditions under which the debris calculation could lead to violation.

## Navigation Warning Track

The warning track was a navigation criterion designed to trap various levels of anomalous implementation of the final trajectory correction maneuver (TCM). The inside boundary of the track was defined as the predicted landing ellipse that accounted for 3-sigma "navigation only" errors while the outside boundary of the track accounted for 6-sigma "navigation only" errors (see Figure C-1). By contrast, the full-up landing ellipse prediction accounted for navigation errors (orbit determination errors, and maneuver execution errors), and atmospheric dispersions. The objective of this criterion was to trap and force disposition of scenarios where the actual TCM implementation was outside of the expected range of performance, even if the full-up predicted landing ellipse was still inside the acceptable region of UTTR.

On Stardust, however, the expected performance of a TCM was very dependent on the execution requirements – size and direction (see Chapter 2). As such, the warning track needed to change

as a function of the "type" of TCM last executed prior to the criteria evaluation. Understanding this characteristic was essential in performing criteria evaluations during a scenario where both the final (E-29 hours) and contingency (E-12 hours) TCMs were required; i.e. the first criteria evaluation (E-21 hours) would use a different warning track than the second criteria evaluation (E-6.5 hours).

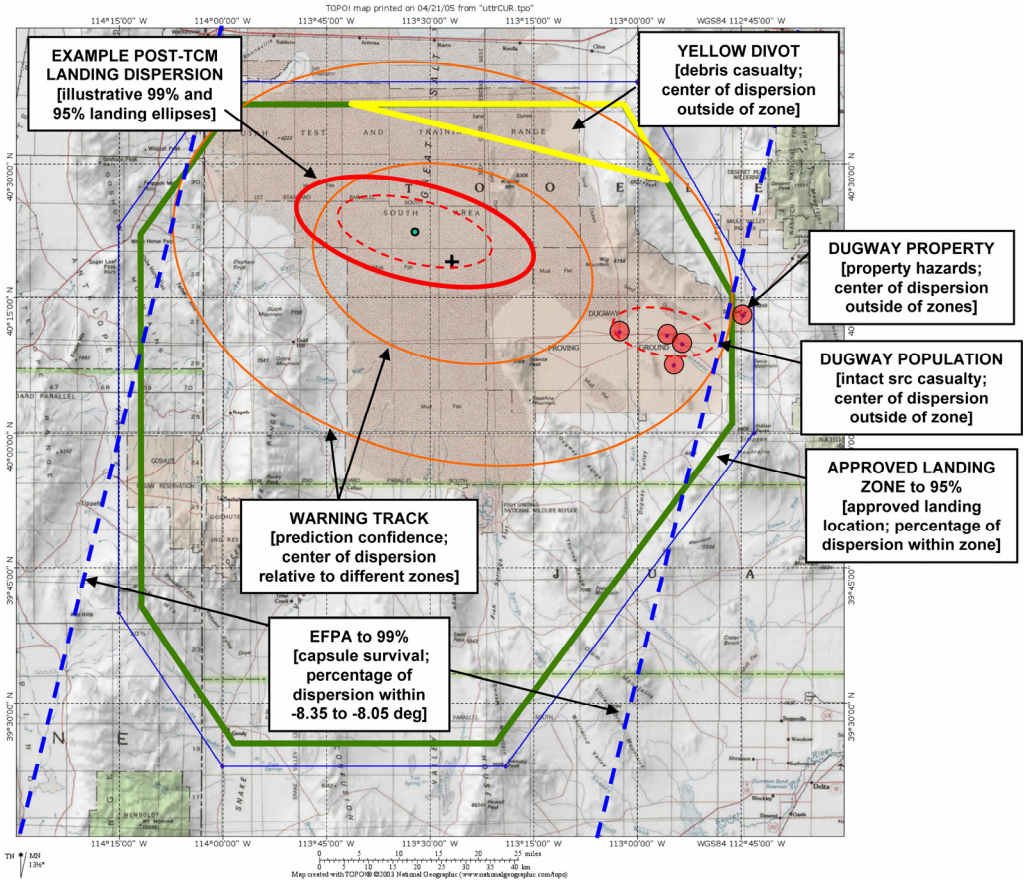



**Figure C-1. Composite Stardust Navigation Criteria**

In addition to the fundamental lesson learned about the connection between the warning track concept and the TCM characteristics, the lack of complete understanding of the criteria construction until late in the test and training process resulted in much confusion and unnecessary debate.

## Capabilities vs. Requirements: Entry Flight Path Angle Criteria

When establishing criteria triggers, it is extremely valuable to know the certified usable limits of parameters being evaluated and not just requirement-based limits. This need was best exemplified on Stardust during the debate, analysis and certification of a wider entry flight path angle (EFPA) corridor (see Chapter 6). During the development phase of the mission, the EFPA error requirement was set at ±0.08° (3-sigma), and the SRC design was verified and validated to this level only (it was after all the era of "faster, better, cheaper"). However, during the Genesis (whose SRC had the same EFPA requirement) and Stardust approach phases, the need for a wider range of EFPA values was discovered during the criteria development and risk assessment process in order to maximize the area within which it was acceptable to land. In fact, the Stardust re-certification effort was initiated formally as a result of a Genesis lesson learned.

With the late addition of the EFPA criterion to the navigation suite and the addition of the anomaly panel, there was significant debate as to the not-to-exceed limits of the EFPA parameter. More thorough and in-depth knowledge of the break point limits of the SRC design, in terms of the EFPA parameter, would have provided significant aid to this discussion and these late adjustments. Key criteria parameters should be identified early in the project's life cycle and consideration given to validation beyond required levels.

## Use of ALL Available Data for Criteria Evaluation

The SRC release enable (green) and disable (red) processes for Stardust (and Genesis) relied primarily on data provided by the project's internal sources: radiometric data, spacecraft telemetry, ground data system and Deep Space Network status queries and checkouts, and visual personnel surveys. A potential source of information for future missions, given the rapid pace of technology, may be independent observation with corresponding trajectory and attitude dynamic evaluation from USSTRATCOM's Space Surveillance Network (SSN), or potentially other providers not known at this time.

This data source was considered for the Stardust (and Genesis) processes, but was discarded due to the forecasted tracking performance, i.e. the SSN assets were predicted to not be able to establish a track until right at (Genesis) or a few hours after the separation event (Stardust). Actual performance was better by several hours. The optical track on Genesis was obtained about 5 hours prior to separation and a radar track about 1.5 hours. On Stardust, the optical acquisition was delayed until there was sufficient sky darkness and occurred only about 50 minutes prior to separation, illustrating that lighting geometry can also play a role in the availability of the data.

A final note – for the proper use of this data, data flow and timelines must not only account for observation time, but also processing of the observations, analysis of the residuals, and communication of results to the decision makers. In addition, the criteria process must be robust to not having this data to evaluate (optical observations can be affected by weather), and to the scenario where the data and/or results are in conflict with the project's data. For the latter, confidence in the robustness and fidelity of the data must be built through end-to-end test and training and independent result validation. For the former, in addition to weather, recognition of USSTRATCOM's role in national security must be taken into account; SSN assets may be re-prioritized with little notice. Open and frequent communications are essential.

## Sample Return Capsule Release Disable Evaluation

The SRC release disable (red button) evaluation process was dependent on indirect or derived parameters as opposed to direct evaluation of driving requirements (risk to population, and property; landing within the approved area). For example, the navigation and spacecraft teams were asked to track and report residuals against the predicted level of velocity change on approach to the SRC release event. This velocity change magnitude was an indication of whether the SRC was on track to land at the predicted location on UTTR. An estimate of the effect of unplanned or erroneously predicted velocity change on the ground location was obtained by using a-priori partial derivatives. These derivatives, however, carried with them assumptions on the nature of the velocity change being applied, in particular the direction of the velocity change. And, while spacecraft attitude was being transmitted to the flight operations team, and was necessarily correct to prevent triggering autonomous fault protection, said attitude was not actively queried during the disable evaluation process.

Although the Stardust event suffered no ill effects from the above construct, future efforts might consider software tools that more directly connect radiometric and spacecraft measurements

through trajectory and EDL simulations into landing site and landing hazard analyses to prevent erroneous evaluation results.

## Safe Mode just prior to Sample Return Capsule Release

The SRC release operation did not directly preclude the possibility of the spacecraft cycling through a safe mode entry, exiting that safe mode (as designed by auto-recovery software), and immediately proceeding to issue the commands for releasing the SRC. The extremely low likelihood of this timing presenting itself instilled confidence in the Stardust approach, in addition to fault protection measures, primarily for the attitude control subsystem, designed to autonomously ensure SRC Release would not proceed, if not proceeding correctly. The nature, size, and hazards associated with the sample being returned may cause future efforts to reconsider this approach and provide for ground interaction.

## Viability of the Backup Orbit Opportunity

The value of the backup opportunity was challenged by various characteristics of the SRC design and its interface with the spacecraft in terms of irreversible or partially irreversible actions taken during the SRC release operation (battery depassivation [defined in Chapter 5], severing of the electrical harness connection). In may be possible to decrease the risk of the backup orbit if these actions and interfaces can be made to retain some level of reversibility.

# Appendix D: Mission Design and Navigation Lessons Learned

There are a number of lessons to be learned from Stardust navigation. Also, it is notable that there was some overlap in the operations teams for Stardust and Genesis, and many of the observations cited here apply to both missions. Therefore, the following should be of considerable interest to future sample return missions. Additional lessons learned with implications on navigation are contained in Appendices E and G.

## Live and Die by Covariances

The Earth return and targeting operation concepts were completely dependent on the navigation statistical covariances. Careful management of the assumptions that go into these covariances was required to perform end-to-end system engineering of the Earth return task. Covariances were key in the evaluation of human and property risk assessment (nominal and debris producing events), landing location success criteria (within approved zone, within expected delivery, "warning track" zones), and recovery operations planning (on flat ground, mountains, minefields, unexploded ordinance, water hazards). For Stardust, these assumptions became very sophisticated and detailed. For example, stochastic models of non-gravitational accelerations included long-term and short-term components, and required months to establish with sufficient fidelity.

The sensitivity of project elements to the navigation model parameters should be well understood. If significant and combined with a lack of confidence in the error modeling, which was not the case for Stardust, consideration should be given to use of other statistical methods, like Monte Carlo simulation.

## Interaction between Navigation and Attitude Control

Overall the two sides of the Rocky Mountains (JPL and LMSS) did an excellent job of communicating. However, as with any long distance relationship, communications can break down if not diligently maintained. The most notable of these breakdowns was regarding the assumptions for trajectory correction maneuver (TCM) execution errors, which led to the maneuver execution error certification process described in Chapter 2.

There were additional minor lapses in communications late in the mission. Attitude changes prior to TCM-18, the penultimate maneuver prior to Entry, were not well propagated, which prompted last minute adjustments to the attitude and small forces models used for orbit determination. Also, the execution of the divert burn was significantly off in direction from that which was modeled (not necessarily unexpected given the change in mass properties as a result of having released the SRC) resulting in the need to do a quick update to the prediction of the trajectory for the Deep Space Network.

Late in the mission, an anomaly occurred in star camera processing. Occasional bad updates were interpreted as attitude errors, large enough to result in the controller commanding thrusters to correct the phantom error. The first of these occurred just after TCM-18, and a sharp-eyed navigator noticed the unexpected change in spacecraft velocity. In order to prevent the problem, the more reliable high-precision mode of inertial measurement unit propagated rates was used for the remainder of the mission. While no ill effects resulted, this problem illustrates the need for careful monitoring and rapid response to anomalies.

It is recommended that the navigation team and the spacecraft team, especially attitude control, meet face to face frequently throughout the mission, on a quarterly basis at a minimum. Navigation and attitude control need to understand one another's processes from end to end

without repeating one another's job. Above all, they should be sensitive to the issues which the alternate team must face.

## Differences in Perception of Navigation Support Required by Project

The importance of navigation in the success of space missions is widely acknowledged, but the staffing levels considered necessary are often a matter of debate. In the era of "faster, better, cheaper" missions, emphasis was often placed on cost savings at the expense of other considerations. For Stardust Earth return, the navigation team evolved from two individuals in January 2005 to 15 or more a year later in the midst of Earth return and recovery events. The need for such a large team can be characterized as a consequence of funding and design decisions made prior to launch. Essentially, one could think of this in the words of a classic television commercial: "Pay me now or pay me later." It is recommended that future low-cost missions demonstrating new capabilities (such as sample return) undertake systematic, end-to-end assessments of mission requirements and capabilities to minimize overall risk and strike a balance between development and operations risks.

# Appendix E: Flight Operations Lessons Learned

By all metrics, the flight operations team accurately delivered a healthy sample return capsule (SRC) to the Earth's atmosphere on the morning of January 15, 2006. The pathway to that delivery, however, was challenged by a few events that could be of interest to future sample return missions. Those events and the lessons learned from them are captured below.

## Low Gain Antenna Multi-Path Impacts

The spacecraft was placed an attitude near the SRC release attitude for the final ten days of the mission. When the spacecraft was placed in this attitude, the telecom carrier strength began to see 10-20 decibel peak-to-peak variations in signal strength. The days remaining until Earth return were spent determining the likely cause of these variations and its impact to the capsule separation events. The most likely cause to the phenomenon was identified as a reflection of the low-gain antenna signal (on the –z-side of the spacecraft, refer back to Figure 1-2) off the bottom of the solar panels and the SRC as a result of the attitude changes made to avoid the Moon as a source of bright body interference (Chapter 7).

The primary impact to operations was a daily loss of telemetry, some of which contained attitude control data necessary for navigation data processing, and loss or degradation of radiometric data during low elevation portions of the Deep Space Network coverage. The decreasing Earth-spacecraft range mitigated the severity of the variations, but the planned communications scheme was modified to use a lower data rate, and/or carrier only tracking to boost signal strength. In addition, lost telemetry were re-transmitted on a daily basis.

Trending and analysis performed during the final few days, along with a continually decreasing Earth-spacecraft range, provided the confidence to proceed with the data rate planned for the range safety and mission success evaluations and general monitoring of the SRC release sequence. However, this antenna performance should have been well characterized during the pre-launch development phase.

## Identification of Critical Telemetry and How to Ensure Receipt

One outcome of the low gain antenna anomaly was the realization that a backup telemetry scheme could be used to provide only the critical SRC release telemetry in response to the possibility of using a much lower data rate. During the week leading up to the SRC release and telecom configuration decisions, a revised telemetry collection scheme was developed, tested and made available for implementation. However, the planned capsule release data rate was used (see previous item) and the revised scheme was not required. The need for an alternate, contingency telemetry collection scheme could have been identified prior to launch and tested during the development phase.

## Sample Return Capsule Battery Telemetry

During the execution of the SRC release activities, the telemetry for verifying that the SRC batteries had been placed on-line with the SRC avionics did not match the expected values. The general contingency response for the SRC batteries not being placed on-line was to swap to the spacecraft B-side and attempt with secondary hardware (Chapter 7), which was not desirable. A real-time evaluation of raw voltage telemetry allowed the flight team to determine that the avionics, batteries, and relays were in the correct state and that the release event should continue without the hardware swap. The source of the anomaly was traced to telemetry measurements that were never fully confirmed during the pre-launch development. Quick

recollection of a review of resistances and voltages during the SRC system review effort (Chapter 6) provided the information required to perform the alternate assessment.

The primary lesson is to confirm all critical telemetry prior to launch. In this case, the SRC battery was a single use component in flight, which should have engendered extra attention. A second lesson is revealed upon further investigation. The uncertainty over telemetry values manifested itself at the start of the SRC release sequence test program, at which point the best estimated telemetry values were coded into the sequence test laboratory simulations. All subsequent testing and operations procedure development used these best-estimated values. The uncertainty over the telemetry values should have been exposed during the risk review process, which could have likely led to establishing the alternate, hardware-based telemetry verification as the baseline in the operations procedure.

# Appendix F: Recovery Operations Lessons Learned

The recovery team planned for, trained and executed the Stardust sample return capsule (SRC) recovery operations flawlessly. The SRC was located in approximately 1 hour against a 20-hour requirement and recovered without incident. Two days later the sample canister and other recovered flight hardware were transported to Johnson Space Center (JSC), where the sample canister was opened and the sample grid handed over to the Science Preliminary Evaluation Team, again without incident. However, during the course of the planning, training and execution of these operations, several lessons were learned which are worthy of capture for future recovery operations.

## Requirements Definition

The requirements imposed on the SRC recovery operations were established 10 years prior to the return event, under the "faster, better, cheaper" paradigm. Due to the Columbia accident and the Genesis SRC drogue release anomaly, there were several additional requirements imposed on the Stardust mission. Other than Genesis Mishap Investigation Board (MIB) findings, these additional requirements were poorly coordinated through formal channels. While a high-level change to the Lockheed Martin Space Systems (LMSS) contract was negotiated and put into action, many of the new requirements were implemented via review findings and action items. Examples are:

1. The SRC Recovery Operations Plan was an LMSS document which did not contractually require NASA or JPL sign-off. In actuality, 7 non-LMSS personnel were required to sign off on the document prior to implementing the plan.

2. Recovery field personnel attire and safety gear became subject to numerous reviews and approvals from NASA and JPL.

3. The NASA Ames Air Worthiness Flight Safety Review and Approval process was not identified until less than a month prior to recovery activity.

## Off-Nominal Recovery Scenario Definition

The off-nominal recovery scenarios that required planning and training were constantly changing based upon the opinions of reviewers with very little filtering as a function of likelihood of occurrence. For example, a scenario was raised in which the SRC landed in the mountains to the west of UTTR and was hot enough to ignite a forest fire. This event required several discussions and was finally eliminated. However, the process took time and effort away from significantly more realistic scenarios. The off-nominal scenarios that the recovery team trained for and were ultimately equipped to handle were determined from the predicted SRC landing locations.

## Sample Return Capsule Landing Location Aids

The SRC was equipped with an ultra high frequency (UHF) beacon, which was activated just prior to landing. While the beacon was detected during SRC descent, reception was spotty after the SRC had landed. The search helicopter was equipped with a thermal imager, but the rapid cooling of the SRC resulted in a thermal signature equivalent to the vegetation on the range. The best aid in locating the SRC, for both training and recovery, turned out to be the parachute canopy. The orange and white canopy was highly visible from the helicopters against the desert background. A consideration for future missions would be either an optical (strobe, especially for

night recovery operations), global positioning satellite broadcast beacon, or a more powerful UHF transmitter.

On the day of Stardust's return, a rather large storm was passing through the UTTR region. Weather conditions were not part of the capsule release criteria because the recovery team was trained for any weather conditions. To aid in locating the SRC, weather balloons were planned at 8 hours and 1 hour before landing, with corresponding updates to the landing predictions. Because of the large storm and a sustained South wind, the 8-hour balloon data predicted capsule landing near a 3-sigma boundary of the planning landing ellipse. The storm began to subside near the time of capsule separation (4 hours from entry) and the decision was made to deploy the second balloon earlier than planned, 3 hours before landing. These data showed that the winds were slowing and that the SRC would land near a 2-sigma boundary; the SRC landed within 1 kilometer (0.5 nautical miles) of this prediction. It is recommended that at least 3 weather balloons be available to support recovery operations and that one be held for one hour before landing. It is expected that the resultant landing location prediction would provide a better predict than the Stardust experience, and, if there were any difficulties with UTTR tracking the SRC to the ground, a more manageable area to search.

As a backup to UTTR tracking, assets provided by USSTRATCOM to track the SRC to the ground were important due to the possibility of bad weather conditions at 3 am in mid-January, in Utah. One of USSTRATCOM's assets (designated System X) was expected to track the SRC to the ground and pinpoint the landing site well within a square mile, but on a best efforts basis. Negotiations with USSTRATCOM settled on no need to call out System X support specifically in the Form 1 documentation. On the day of return, however, System X became unavailable to the project, with little warning or explanation. Future projects wanting such backup might consider formalizing the use of System X with USSTRATCOM or developing alternate contingency plans for locating the SRC in the absence of UTTR tracking.

## Field Video Coverage

The SRC Recovery Plan included the presence of a video camera on-scene to record the recovery field operations and provide real-time coverage to the Recovery Command Center. A relay antenna was placed on a local mountain to support relay of the video back to the command center but, when the Blackhawk helicopter was reassigned, the backup helicopter was not large enough to carry the video equipment in addition to recovery personnel and the on-scene video camera was not used during actual recovery operations. Future projects may wish to revisit the use of an on-scene camera.

## Sample Return Capsule Processing Timeline

The recovery team had 2 days for processing the recovered SRC prior to transporting it to JSC. At least one more day should be allocated for future missions. Many of the personnel at UTTR for the recovery were required to be at JSC to receive the SRC. This necessitated their departure from UTTR the day after recovery leaving a skeletal team behind to conclude the preparation procedure. Having an extra day between recovery and transporting would have significantly relieved the stress level for the team.

## Public Affairs and Visitor Interactions

The Stardust Project underestimated the amount of time and effort required by recovery team members to support public affairs functions (Figure F-1). Future missions should allocate more

time for media viewing of the returned hardware. Having additional time between recovery and transport (previous item) would help in this regard.

**Figure F-1. Accommodating Significant Media Interest**

In addition, the project made an effort to support program, project and other visitors who desired to be at UTTR for the Earth return and sample recovery. However, surveys taken months before return yielded very little interest and the project did not pursue using additional facilities (the nearby Cuddes building) that could have been equipped with voice and video communications capability. In the final weeks preceding the return, tens of people expressed a need to be at UTTR and many of them could not be accommodated. Future missions should coordinate early with relevant public affairs personnel to consider setting up additional facilities for these visitors even if they end up being underutilized, thus keeping the Recovery Command Center less congested. The use of special badges to control access was also very useful as visitors wanted to be where there was action, forgetting that they were on a highly secure military base and potentially interfering with critical operations.

## Risk Communication with the Local Population

In addition to the risk communication tasks described in Chapter 9, the risk communication efforts on Genesis and Stardust benefited from the following key lessons in the dissemination of information to local communities near the UTTR landing site. First and foremost, the NASA HQ Office of Legislative Affairs was very instrumental in scheduling group legislative briefings with local senators' and the governor's offices.

Other effective means of distribution were found to be briefings at local newspaper editorial board meetings and the local chambers of commerce, and distribution of reading materials at high trafficked city hall and local libraries. Local schools were found to only take material distributed

by the district office; one visit to the local superintendent's office was the most effective way to reach the educational community. Finally, information transfer and briefings to local Native American tribes was best coordinated through the Bureau of Indian Affairs.

For training UTTR personnel, the Dugway Proving Grounds public affairs organization distributed mission background and risk information prepared by NASA and JPL.

# Appendix G: Vehicle Design Lessons Learned

The Stardust spacecraft and sample return capsule (SRC) were designed to navigate to Comet Wild 2, capture comet particles from the coma during flyby, survive passage through the coma and return the comet particles to Earth. It was designed in a very tightly constrained design-to-cost environment to meet the Discovery 4 total mission cost limit of $164 million (the rest of the $200 million was for the launch vehicle). The mission had previously been conceived as requiring several hundred million. No extras could be afforded. In addition to the vehicle design lessons learned that can be inferred from the main body of this document, the following paragraphs describe additional lessons learned that derive from the specific Stardust design implementation.

## Unbalanced Thrusters

The comet encounter configuration was shown in Figure 1-2. For encounter, the aerogel was folded out from the SRC, above the whipple shield extension that protected the high gain antenna feed. The solar array whipple shields protected the tail end of the arrays from dust for up to a 2º attitude excursion. A prime science requirement was to avoid hydrazine plume impingement and contamination of the aerogel with material that could confuse science analysis after return. To meet this requirement, three-axis attitude control was implemented with all thrusters on the bottom (-z side) of the spacecraft. In addition, to protect against a large particle (rock) deflecting the attitude beyond a 2º attitude excursion, four 1-pound (4.4-Newton) thrusters were provided to apply maximum torque from dual strings to rapidly restore the spacecraft attitude after particle impact and minimize exposure of the spacecraft to the dust stream.

The unbalanced thruster configuration was established during early preliminary design along with a navigation requirement to deliver the spacecraft to the Earth with an entry flight path angle error of ±0.06º (the remaining ±0.02°, for a total allowed error of ±0.08°, was allocated to the SRC release mechanism and spacecraft performance). As the mission progressed, the small force errors resulting from this unbalanced configuration became better understood and a concern developed regarding the ability to meet the return targeting requirements, see the discussion in Chapter 2.

While both Genesis and Stardust demonstrated that one can successfully navigate to a precise Earth entry, in hindsight it is evident that the unbalanced configuration for thrusters led the project to accept additional operations cost and residual risk to mission success. This is not to say that unbalanced thrusters could never be flown accurately. For instance, momentum wheels, fuel tank bladders or single-axis slew schemes could have gone a long way towards reducing risk. However, the problem may have been more with the development of requirements than with the actual spacecraft design. Recall that the maneuver requirements had incomplete definitions prior to launch. One solution might have been to have taken the time to specify maneuver requirements completely (slew and burn), followed by allowing spacecraft designers to come up with the system to meet such requirements. Repeatability and predictability of performance are also important considerations, in addition to meeting requirements. For example, a design solution that could have been implemented was one-sided thrusters through the sample collection to meet the science contamination avoidance requirement together with a balanced set of thrusters that could have been used after sample collection. This kind of design was not selected for Stardust because of the severe mass constraint and the extremely tight cost constraints.

Beyond the spacecraft design itself, as a mitigating factor for risk, biasing of maneuvers can be applied to constrain possible maneuver directions. Moreover, deadband walks of three-axis spacecraft with unbalanced thrusters are preferable to slews when setting up maneuvers. Deadband walks entail turning (or performing attitude maneuvers) at a slower rate, moving the deadbands within which the attitude is maintained via limit cycling, at rates on the order of degrees per minute instead of degrees per second. Fixed attitude maneuvers (if you can perform

them) mitigate the need to have walks or slews and are better yet. Furthermore, robust propellant margins can compensate for effects of biasing maneuvers. However, the implications of imposing operational constraints should be weighed carefully against spacecraft design decisions to ensure a proper balance of risk and cost.

## Sample Return Capsule Thermal Protection System

The fact that the SRC entry was going to be the fastest Earth entry to date posed an incredible challenge to the thermal protection system design. At the time of the 1994 Stardust Mission proposal, the challenge of identifying a heatshield material that could withstand such a harsh environment was daunting. The predicted peak heat flux for the SRC entry exceeded the performance capabilities of the thermal protection systems (TPS) available at the time, except for one: conventional fully dense carbon phenolic. Carbon phenolic was widely used for Department of Defense (DoD) ballistic entry applications and was the heatshield for the Galileo entry probe into Jupiter, under heating conditions 30 times more severe than the Stardust SRC entry. It certainly could have been a candidate. Its downfall was that its density was 1.4 grams per cubic centimeter (0.05 pounds per cubic inch), which would have pushed the mass of the SRC over that available to meet launch constraints. Use of the Apollo Avcoat ablator was also considered, but the Stardust entry heating rate was substantially higher than its qualification limit. Without a lighter heatshield candidate, the feasibility of proposing such a lightweight SRC would be difficult.

During the pre-proposal feasibility assessment phase, LMSS approached NASA Ames Research Center (ARC) to learn more about their newly-developed lightweight ceramic ablator class of materials. One of the materials was slated to fly on the Mars Pathfinder mission, and another, phenolic impregnated carbon ablator (PICA), was showing great promise in arc jet tests. The material had been successfully tested at heat fluxes representative of SRC entry predictions, with a density six times less than fully dense carbon phenolic. The material had only recently been invented and was at a relatively low Technology Readiness Level (TRL), however there was enough data to show feasibility for flight. A Space Act Agreement was established between ARC and LMSS in 1995 to scale-up the material process to produce a single-piece, full-scale mock-up SRC heatshield to support the Phase A study and the proposal to implement the program. LMSS established a subcontract with Fiber Materials, Inc. (FMI), who had supported ARC in the PICA research, to manufacture the heatshield.

Once Stardust was selected, tasks were initiated to simultaneously perfect the scale-up process into a single-piece heatshield, and to qualify PICA for flight with arc jet tests and a representative computational thermal model. Each of these areas posed significant challenges, especially in the “faster, better, cheaper” environment. However, the material went from a relatively low TRL to delivery of flight heatshields in two years, unprecedented in the typical TPS development to flight cycle. Working with FMI and Ames during those two years, a workable flight heatshield system based on PICA was achieved that met LMSS’s repeatable manufacturing specifications.

The aerothermal environment prediction methodology, coupled with the PICA thermal response model, was groundbreaking at the time. A team consisting of LMSS staff, NASA Langley Research Center experts, and NASA Ames Research Center aerothermodynamic and material experts, developed innovative methodologies for modeling and simulations of the SRC Earth entry condition. This was the first time that high-fidelity flow calculations, with coupled radiation and ablation, were used as the primary tool for a heatshield design. The NASA Ames team developed an innovative TPS sizing code, named Fully Implicit Ablation and Thermal Analysis Program (FIAT) in less than six months, and later extended it to a 2-dimensional code. This innovative approach is now a standard for planetary entry aerothermal environment CFD predictions.

Existing flight data to date was so sparse that the aerothermal and TPS community added significant margin to the TPS design, i.e. added weight to the spacecraft. In some locations on

the SRC afterbody, the TPS design included an assumed environment triple the CFD predictions due to the large prediction uncertainties as well as unassessable parameters such as lower afterbody radiation heating. In order to validate these tools, an attempt was made by ARC to include instrumentation in the SRC TPS to take advantage of the unique opportunity of being the fastest Earth entry to date (see TPS instrumentation lesson learned below).

The SRC design analyses bounded the entry parameters with proper consideration for the fact that the new PICA heatshield material had only been built and tested in small test coupons at the time the design had to be established. The low density of the PICA was an enabler for the extremely mass constrained mission (PICA is about half the density of the Apollo Avcoat ablator).

## Entry Flight Path Angle Accuracy

An entry flight path angle (EFPA) of -8.2º was a good compromise to balance heating rate and total heating, both critical parameters in qualifying the PICA for the highest velocity entry of any man made object. A key parameter in constraining the heating rate and the total heating of the PICA was the entry flight path angle, which was set at -8.2º ±0.08º during development. The tolerance was divided arithmetically ±0.06º for navigation and ±0.02º for the spacecraft. Since both the spacecraft and navigation teams believed during development that they could meet their respective tolerances, the analyses and testing performed for entry and the performance of the PICA were based on limiting the entry flight path angle to the range of -8.12º to -8.28º. As entry was approached and concern grew over the ability to navigate to this tight tolerance an investigation of the criticality of this tight EFPA was performed. This investigation was described in Chapter 6.

The bounding analyses performed during development had to be accomplished before the mass of the SRC was known and before the testing of the PICA was completed. Rerunning of selected PICA ablation performance analyses by ARC, assessment of all the PICA test data including retesting performed in 2000 after a challenge to pre-calibrations resulted in ARC management invalidation of the data, and rerunning of the Langley Research Center 6-degree-of-freedom entry analyses showed that there were no ‘cliffs’ at either end of the EFPA range. These bounding analyses were very effective in providing adequate margin to broaden the EFPA during the last few months before entry. The Stardust budgets were so tight that there was no plan to rerun the analyses after the build was completed. In future programs, it would be prudent to budget rerun of the entry and heatshield performance analyses after the final hardware parameters are known to accurately determine the margins prior to launch and as entry approaches. It would also be prudent to perform parametric analyses to fully understand the bounds of performance and maximize flexibility for the operations team as they finalize the entry trajectory and SRC release plans.

## Thermal Protection System Instrumentation

From the viewpoint of the entry, descent, and landing community the Stardust SRC presented an opportunity to obtain much needed high value data on vehicle and TPS material performance. The lack of hard, experimental data necessitated inclusion of large margins in capsule design to cover uncertainties in aerothermal modeling and material performance modeling. ARC proposed, first to the Stardust Project, and then to NASA HQ, that instrumentation be added to the Stardust TPS to obtain a basic data set during Stardust entry.

The Stardust Project was focused on cometary particle return and meeting the cost commitments made in the original proposal. While the required instrumentation cost would have to be added to the project by NASA, instrumenting the heatshield would have also introduced an unknown risk to an already challenging development. The proposal was not viewed favorably and NASA HQ

decided to not provide the required financial resources. The opportunity to validate the TPS design tools was lost along with the possibly of reducing design uncertainties for future missions.

A lesson learned from this experience might be that if technology-enhancing opportunities such as this one are to be encouraged, then a process might be defined that does not add risk to the mission. One approach might be a separately funded study that parallels Phase B such that the preliminary technology design could be developed along with resource estimates for both the technology inclusion and the delta cost to the mission for mitigation of any risk added.

## Sample Return Capsule Ballast Mass

To meet aerodynamic stability requirements, the SRC's center of gravity (c.g.) had to be located along the spin axis no further from the stagnation point than 0.351 of the capsule maximum diameter. In addition, the design of the SRC was driven to maximize the size of the aerogel tray by locating it at maximum capsule diameter. However, after incorporating the parachute at the top end and the battery and electronics on the deck, the c.g. was too far from the nose. It was necessary to add ballast in the nose of the capsule to achieve the necessary separation between the c.g. and the center of pressure. A plate was designed with eight tungsten blocks located as far forward in the nose as possible.

During analyses of the failure scenarios that could result in an uncontrolled entry of the capsule, i.e. those performed in support of the range safety analysis described in Chapter 3, the breakup and burnup analyses showed that only the tungsten ballast and the heatshield would survive to the ground. To aid compliance with range safety requirements, lead could have been selected for the ballast mass at a penalty of 2.8 kilograms (6.2 pounds), which was significant during Stardust design. Lead would have completely vaporized during the proposed scenarios. During Stardust development phase, the analyses required for compliance with range safety had not been envisioned; only a top-level burnup analysis was done. Now that these analyses are known, future programs should plan for completion of breakup and burnup analyses during the design phase so that design impacts can be considered while they can be implemented.

# Appendix H: Pre-Launch Project Life Cycle Observations

The Stardust Project successfully added risk assessments, analyses and reviews in the year before return that had not been foreseen during development and had not been included in the operations phase cost estimates. Many of the activities performed in the last year before Stardust return could be accomplished much more efficiently if performed during the development phases. They would benefit from this time when all the hardware experts are accessible to the project. With relatively little additional effort, these assessments would then be reviewed for changes that had occurred during the flight prior to Earth return mission operations.

For example, pre-launch Stardust analyses for entry were performed with the goal of establishing design parameter bounds such that it would be clear, when the design and build had been completed, that if all the sample return capsule (SRC) flight parameters stayed within the established bounds, the SRC would operate correctly; it was flying inside the "box". It was acceptable to not quantify margins; recall that Stardust was designed and built during the "faster, better, cheaper" era.

The new risk assessment paradigm required analyses and margin determination for the "as-built" conditions. Implementation of this paradigm during the development phase might include the following activities:

- Bound design parameters for the reasonable ranges of parameters during Phase B
- Perform point analyses during Phase C, when design parameters are known, along with sensitivity analyses to understand where in the 'box' the point design is located,
- Update the point design and sensitivity analyses during Phase D, when hardware actuals and test results are known, to understand margins and break points.

Completion of these activities during the pre-launch phase would also aid in the management of independent review boards. As many projects do, Stardust used a standing review board during development whose members became familiar with the design, trades, decisions and performance predictions as the project evolved. With the addition of new detailed reviews, 6 years after launch, it was impossible to reconstitute the development phase standing review board and there was very little participation from the development era board. The initial Earth return review process was spent in educating new review participants with a tendency toward design, as opposed to risk, on hardware that had been launched over six years before.

Using the current knowledge of the NASA return requirements, all elements of the return plans, procedures, decision trees and risks can be completed prior to launch when all the expertise is available to the project. As with the hardware review process, in the months prior to return the reviews can focus on the changes that come out of the knowledge gained from operating the system throughout the mission. The review plan for the months leading up to return should be defined during development along with appropriate cost estimates. A recommended suite of pre-return operations reviews might be:

- Element risk reviews, focusing on changes and lessons learned since launch
- Project risk review, again, focusing on changes and lessons learned since launch
- Element readiness reviews
- Project readiness review
- Senior Management readiness reviews

To minimize the cost of the Earth return assessments, it is necessary to archive the analyses, memoranda, review presentation material, plans, procedures, training records, etc. for return and recovery since they will have been dormant for the mission duration until return preparations get

underway. Stardust used replicating servers during development, and a web-based docushare system after launch. Archiving was not at the forefront of this design and many files became unreadable as commercial-off-the-shelf applications were upgraded. With the rapidly advancing web based sharing tools, a complete record system accessible to all project participants, with an eye toward archiving, must be set up prior to launch and be preserved for the return and recovery phase.

The remainder of this appendix describes lessons learned, not necessarily applicable to the final year of Stardust operations, but nonetheless valuable during the pre-launch phases of a sample return mission.

## Selection of the Landing Location

The landing location is an early decision since it is significant to mission design, compliance with environmental laws, return analyses, and recovery planning. During the parallel Phase A studies of Stardust and Genesis (which was Suess Urey in that first competitive down select), Wallops Island, White Sands and the Utah Test and Training Range (UTTR) were seriously considered for return and recovery.

The Wallops Island range is operated by Goddard Space Flight Center, which would make coordination easier as a NASA range. However, Wallops is an ocean range and would have required the SRC to be designed for water landing, adding the serious complication of sealing the entry pressurization vents, or sealing the capsule itself with the attendant mass penalty to withstand the pressure differential from vacuum to a full atmosphere. Another issue with Wallops was the lack of a tracking infrastructure that could pinpoint the landing location within the 80 x 30 kilometer (43 x 16 nautical mile) estimated landing footprint. The tracking requirements could have been met by the Navy, but even in the pre-full-cost-accounting days, this was estimated to be a major fraction of the total $200 million cost cap for Discovery 4. On the other hand, White Sands was found to be a very capable range with full infrastructure for tracking and locating the capsule, but it runs primarily North-South while the Stardust landing ellipse was predominantly East-West. The anticipated landing ellipse at White Sands also encompassed mountains.

The UTTR had the extensive infrastructure needed for tracking (UTTR can track and support dog fights of 50 aircraft while keeping them at safe distances and scoring their performance) and had the required East-West real estate to easily contain the footprint. In addition, UTTR controlled the airspace over the range to an altitude of 17,700 meters (58,000 feet), greatly simplifying the coordination for entry since the SRC's entry trajectory was such that it would decelerate, turn, and drop into the range almost vertically. Without this characteristic, Stardust would have been required to coordinate with air traffic control on its own, a significant additional cost. Formal coordination with UTTR started during Phase B based on a NASA and Department of Defense Memorandum of Agreement (MOA). Subsequent interaction was described in Chapters 9 and 10.

During the Earth return preparation reviews, board members and other participants kept bringing up "why not water landing", "why not Australia", "why not the Sahara desert", "why not the steppes of Russia", "why not the farmlands of Kansas". In addition to the advantages described above, the Genesis and Stardust experiences show how safety is now known to be paramount. Controlled, unpopulated ground space allowed Stardust to safely return the capsule while meeting range safety requirements. In addition, landing at UTTR allowed the staging of all recovery personnel outside the landing footprint. UTTR is hard to beat as a great location with all the required space, infrastructure, trained personnel, and range and airspace control not to mention all of the MOA's in place with NASA. Also, the land is relatively flat, the soil is soft, and it has the largest restricted air space in the contiguous United States.

## Entry, Descent, and Landing and Thermal Protection System Analyses

The mission design dictates the direct entry velocity. Stardust traveled half way to Jupiter and its entry velocity was high, 12.8 kilometers per second (28,600 miles per hour). Genesis went to an Earth-Moon libration point, only about one million miles from Earth, so the entry velocity was only 11.0 kilometers per second (24,600 miles per hour), only slightly higher than lunar trajectory return velocities. Lifting entry, such as Apollo, could limit entry deceleration, but requires an active descent control system, which is typically not in the budget for a low cost mission. It might also be possible to perform aerocapture or aerobraking to reduce the entry velocity, but this would introduce additional trajectory control challenges.

Posigrade (with Earth's rotation) versus retrograde entry can be selected with small impact on propellant. However, the additional 0.7 kilometers per second (1560 miles per hour) velocity relative to Earth's rotating atmosphere is significant to the capability requirement for the heatshield since entry heating goes roughly with the cube of velocity. This is not a trivial difference. Early in Stardust development it was decided that posigrade entry was appropriate, particularly with a new, unproven heatshield. Although this also lead to a night recovery, which would be a little more challenging, it was agreed that the a little delay until daylight, if the capsule was not found in the dark, was a small part of the allowed recovery time (then 40 hours).

Entry flight path angle (EFPA) is the next most significant decision to be made during the development phase. Too shallow and the capsule skips out, steeper than about 6º is needed for a predictable entry trajectory. Then it is a matter achieving a balance between of trajectory accuracy, heating rate and the total heat load. Steeper entries push toward material heating rate capability limits while shallow entries result in longer entry and greater total heating, also stressing heatshield material but also affecting heat soak into the interior of the capsule. The heatshield manages the high heat rate by ablation while the thickness of the material acts to minimize thermal conductivity into the structure and the interior of the capsule. For Stardust and Genesis the design sweet spot selected was -8.2º. For further discussion of the EFPA accuracy trade space see Appendix G, Vehicle Design.

## Sample Return Capsule Design

Capsule shape was based on shape studies and testing performed for the Viking program. The conical heatshield and backshell shape determines supersonic stability. Blunt conical capsule configurations are stable at hypersonic and supersonic speeds, but are unstable at subsonic speeds. In one wind tunnel test the Stardust capsule inverted and stabilized upside down; a poor attitude for parachute release. Early in the design process, the capsule stability was tested in the Eglin Air Force Base shadowgraph tunnel to determine low supersonic stability and establish the velocity at which a stabilizing drogue parachute should be released. The Stardust SRC shape was verified to be stable down to Mach 1, so the drogue release was set at Mach 1.4 to provide good margin. The potential variation in g-triggering was found to provide drogue release in the range of Mach 1.2 to 1.6. The Genesis biconic backshell configuration also showed potential instability onset approaching Mach 1.2, so the drogue chute release was set higher at Mach 1.6 (Mach 1.4 to 1.8).

The simple design selected to perform the parachute deployment was the G-trigger and timer combination described in Chapter 5. A Pitot tube that could survive entry and not interfere with capsule aerodynamics would be a design challenge. Inertial measurements units to measure deceleration and a processor to integrate along the trajectory would add costs well beyond affordability for a project with a cost cap of $200 million. The parachute release timing was based on completion of hypersonic deceleration. Three-G's of deceleration was at the knee of the time history curve and was a good detectable point to start the timers. The time from that point to

Mach 1.4 was based on the 6-degree-of-freedom entry trajectories run by NASA Langley Research Center. Drogue chute release spanning Mach 1.2 to 1.6 provided adequate margin above instability and parachute inflation loading at the high end. These parameters were established early in Phase C to support purchase of the acceleration switches and the design of the timer circuit. The mechanical moving mass acceleration switches that were used are simple and reliable. These, in combination with simple resistor-capacitor timer circuits, were a straight forward design for the entry, descent, and landing (EDL) functions.

TPS thickness had to be established early enough in the detailed design to allow fabrication time for the heatshield and backshell. Trajectory analyses at Langley, TPS performance analyses at LMSS for the backshell, and at Ames for the heatshield established the expected heating rate, total heating, ablation pyrolysis zone depth and recession. A thermal model provided the soak back heating of the capsule interior. Margins were applied to account for the many uncertainties in all of the entry parameters and the material performance properties.

Since this was an SRC design from scratch, a Structural Thermal Model (STM) (qualification unit) was fabricated and tested ahead of the flight SRC. Heatshield fabrication proved to be challenging and the STM had to proceed into test before a heatshield was built to the required density and uniformity requirements. The flight heatshield required many fabrication attempts and pushed the flight SRC schedule to just about the limit, affecting completion of SRC testing and delivery to the spacecraft integration and system testing. Stardust's 28 months from confirmation to launch was a tight schedule, especially for a brand new SRC design. A longer schedule would be prudent but if not available getting the EDL and SRC design decisions firm in Phase B or very early in Phase C is critical.

# Appendix I: Acronym List

| | |
|---|---|
| ° | degree (angular or temperature) |
| 1SPCS | 1st Space Command Squadron |
| ACS | attitude control system |
| AFB | Air Force Base |
| AFSPC | Air Force Space Command |
| ARC | Ames Research Center |
| ASL | above sea level |
| ATC | Air Traffic Control |
| AU | astronomical unit, or 1.49597870 x $10^{11}$ kilometers |
| AU | avionics unit |
| C | centigrade (temperature) |
| C&DH | command and data handling system |
| c.g. | center of gravity |
| CA | California |
| CAIB | Columbia Accident Investigation Board |
| CAPTEM | Curation and Analysis Planning Team for Extraterrestrial Materials |
| CC | cable cut |
| CCT | Contingency Coordination Team |
| CDR | Critical Design Review |
| CERR | Critical Events Readiness Review |
| CFD | computational fluid dynamics |
| Cine-T | Cinetheodolite (visual tracking system) |
| cm | centimeters |
| Cmd | command |
| CMOC | Cheyenne Mountain Operations Center |
| CoCER | Certification of Critical Event Readiness |
| conj | conjunction |
| COORD | coordination |
| DC | De Havilland Comet (aircraft series designation) |
| DC | District of Columbia |
| DF | direction finder |
| DISA | direct inward system access |
| DoD | Department of Defense |
| DPA | destructive physical analysis |
| DSN | Deep Space Network |
| dyn | dynamics |
| E | Earth |
| EA | environmental assessment |
| ECC | emergency control center |
| EDL | entry, descent, and landing |
| EFPA | entry flight path angle |
| EOD | explosive ordinance disposal |
| ETESP | Earth Targeting and Entry Safety Plan |
| F | fahrenheit (temperature) |
| FAA | Federal Aviation Administration |
| FEMA | Federal Emergency Management Agency |
| FIAT | Fully Implicit Ablation and Thermal Analysis Program |

| | |
|---|---|
| FMI | Fiber Materials, Inc. |
| FPGA | field programmable gate array |
| FS | flight system |
| FTP | file transfer protocol |
| G | unit of acceleration due to gravity on the Earth's surface, or 9.81 $m/s^2$<br>g-force is a force equivalent, 9.81 N/kg |
| GB | green button (meeting) |
| GDS | ground data system (team) |
| $GN_2$ | gaseous nitrogen |
| G-switch | acceleration sensing switch |
| h | hour |
| HCAC | Headquarters Contingency Action Center (NASA) |
| HQ | headquarters |
| ICS | Incident Command System |
| IIP | instantaneous impact point |
| IMU | inertial measurement unit |
| IR | infra-red |
| IRT | Independent Review Team (for recovery operations) |
| ISR | intelligence, surveillance, and reconnaissance |
| ITL | incompressible test list |
| J38 | Joint Staff / Space and Missile Operations |
| J5 | Joint Staff / Plans |
| JPL | Jet Propulsion Laboratory |
| JSC | Johnson Space Center |
| km | kilometer |
| LaRC | Langley Research Center |
| LFACC | Lead Federal Agency Contingency Coordinator |
| LMSS | Lockheed Martin Space Systems |
| m | meter |
| MAAF | Michael Army Air Field |
| MATTRACKS | rubber track conversion system, industry supplier |
| MCC | Mission Control Center (at Hill AFB) |
| MDS | mission data system |
| MER | Mars Exploration Rover |
| MIB | Mishap Investigation Board (Genesis) |
| mm | millimeter |
| MM | Mission Manager |
| MOA | memorandum of agreement |
| MOA | mission operations assurance |
| MOS | mission operations system (team) |
| MOSFET | metal-oxide semiconductor field-effect transistor |
| MOU | memorandum of understanding |
| MSL | mean sea level |
| NASA | National Aeronautics and Space Administration |
| NAV | navigation team |
| NEO | Near Earth Orbit (Observation Team) |
| NEPA | National Environmental Policy Act |
| NIRSPEC-c | Near Infrared Spectrometer instrument |

| | |
|---|---|
| NLO | NASA Liaison Officer |
| NORAD | North American Aerospace Defense Command |
| NORTHCOM | United States Northern Command |
| NSI | NASA standard initiator |
| | |
| OD | orbit determination |
| OIA | operations interface agreement |
| Ops | operations |
| ORT | operational readiness test |
| OSCAR | On-scene Commander |
| OSMS | Office of Safety and Mission Success (at JPL) |
| | |
| PABX | Private Automatic Branch Exchange |
| PAD | Packet Assembler – Disassembler |
| PET | Preliminary Evaluation Team |
| PICA | phenolic impregnated carbon ablator |
| PID | Program Introduction Document |
| PIM | pyrotechnic initiator module |
| PM | Project Manager |
| POTS | plain old telephone service |
| PPAC | Planetary Protection Advisory Committee |
| PPE | personal protective equipment |
| PPO | Planetary Protection Office |
| proc | procedure |
| PSTN | Public Switched Telephone Network |
| | |
| QA | quality assurance |
| | |
| R&R | release and retention |
| RAS | restricted airspace |
| RCS | Recovery Command System |
| REC | recovery operations |
| ref | reference |
| Rel | release |
| RF | radio frequency |
| RFA | request for action |
| RM | Recovery Manager |
| ROI | region of influence |
| | |
| s | second |
| S/C | spacecraft |
| SAD | Space Analysis Division |
| SCT | spacecraft (team) |
| SDU | Stardust |
| SEH | Space Exposed Hardware (Laboratory) |
| SMA | Safety and Mission Assurance |
| SMARR | Safety and Mission Assurance Readiness Review |
| SMD | Science Mission Directorate (NASA Headquarters) |
| SMSR | Safety and Mission Success Review |
| SOC | Statement of Capability |
| SPF | single point failure |
| SRB | Safety Review Board (at UTTR) |
| SRC | sample return capsule |
| SRPH | Sample Return Primer and Handbook |
| SSN | Space Surveillance Network |
| STL | spacecraft test laboratory |

| | |
|---|---|
| STM | structural thermal model |
| STRATCOM | United States Strategic Command, also USSTRATCOM |
| TCM | trajectory correction maneuver |
| TPS | thermal protection system |
| TRL | technology readiness level |
| | |
| UH | Utility Helicopter (helicopter series designation) |
| UHF | ultrahigh frequency |
| USSTRATCOM | United States Strategic Command |
| UTC | universal time coordinated |
| UTTR | Utah Test and Training Range |
| | |
| VOCA | voice operational communications assembly |

# Appendix J: References and Project Library Contents

## References:


1. Columbia Accident Investigation Board (2003). Columbia Accident Investigation Board Report Volume 1. National Aeronautics and Space Administration.

2. Genesis Mishap Investigation Board (2005). Genesis Mishap Investigation Board Report Volume 1. National Aeronautics and Space Administration.

3. Genesis Mishap Investigation Board (2006). Genesis Mishap Investigation Board Report Volume 2. National Aeronautics and Space Administration. (Not in compact disk library as not yet released)

4. C. L. Potts and P. R. Menon, "A Priori Stochastic Non-Gravitational Acceleration Effects on Stardust Navigation Earth Entry Covariance," JPL Interoffice Memorandum 312.H-00-001, March 9, 2000. (JPL Internal Document).

5. K. E. Williams, B. M. Kennedy and E. Carranza, "Report on Stardust 1-AU Calibration Activities," JPL Interoffice Memorandum 312.G-03-021, October 6, 2003 (JPL Internal Document).

6. B. M. Kennedy, E. Carranza and K. E. Williams, AAS 04-134, "1-AU Calibration Activities For Stardust Earth Return," 2004 AAS/AIAA Space Flight Mechanics Meeting, February 8-12, 2004.

7. B. Kennedy, T. McElrath, and S. Nandi, AIAA-2006-6408, "Modeling of Deadbanding Delta-V for the Stardust Earth Return: Calibration, Analysis, Prediction and Performance," 2006 AIAA/AAS Astrodynamics Specialist Conference, August 21-25, 2006.

8. S. Nandi, B. Kennedy, K. Williams, and D. Byrnes, AIAA-2006-6409, "On Orbit Maneuver Calibrations for the Stardust Spacecraft," 2006 AIAA/AAS Astrodynamics Specialist Conference, August 21-25, 2006.

9. Stardust Navigation Plan, January 20, 1999 (JPL Internal Document).

10. C. Helfrich, R. Bhat, J. Kangas, R. Wilson, M. Wong, C. Potts, and K. Williams, AIAA-2006-6406, "Maneuver Analysis and Targeting Strategy for the Stardust Re-Entry Capsule," 2006 AIAA/AAS Astrodynamics Specialist Conference, August 21-25, 2006.

11. P. Desai, D. Lyons, J. Tooley, and J. Kangas, AIAA-2006-6410, "Entry, Descent, and Landing Operations Analysis for the Stardust Re-Entry Capsule," 2006 AIAA/AAS Astrodynamics Specialist Conference, August 21-25, 2006.

12. D. Jefferson, D. Baird, L. Cangahuala, and G. Lewis, AIAA-2006-6411, "Interfacing with USSTRATCOM and UTTR During Stardust Earth Return," 2006 AIAA/AAS Astrodynamics Specialist Conference, August 21-25, 2006.

13. J. Tooley, P. Desai, D. Lyons, E. Hirst, T. Wahl, M. Ivanov, and G. Wawrzyniak, AIAA-2006-6412, "Landing and Population Hazard Analysis for Stardust Entry in Operations and Entry Planning," 2006 AIAA/AAS Astrodynamics Specialist Conference, August 21-25, 2006.

14. D. Baird, S. Bhaskaran, M. Jah, D. Jefferson, B. Kennedy, G. Lewis, T. Martin-Mur, T. McElrath, N. Mottinger, S. Nandi, and P. F. Thompson. "Stardust Earth Return Orbit Determination," Unpublished Paper (JPL Internal Document), August 2006.

15. Range Safety Program, NASA Office of Safety and Mission Assurance, July 8, 2005. NPR 8715.5.

16. Range Commanders Council Standard: Common Risk Criteria for National Test Ranges, Subtitles: Inert Debris, June 2002. RCC-STD 321-02.

17. Guidelines and Assessment Procedures for Limiting Orbital Debris, August 1995. NSS 1740.14.

## Project Documentation (Return Phase)

| | **Project Area:** | **Systems Engineering** |
|---|---|---|
| | File Location: | / Project-Documents / System-Engineering / |
| REF | Document Name | File Name |
| S1 | Certificate of Critical Event Readiness (CoCER) for Earth Return and .. | Certificate-Of-CER |
| S2 | Earth Targeting and Entry Safety Plan Volume 1: Safety Analysis | ETESP-Volume1 |
| S3 | Earth Targeting and Entry Safety Plan Volume 2: Decision Criteria | ETESP-Volume2 |
| S4 | Genesis MIB Board Recommendations to Stardust Mission | Gns-MIB-Recommendations |
| S5 | Probabilistic Risk Assessment (PRA) Logic Model:<br>Probabilistic Risk Assessment (PRA) Logic Model Memo<br>Master Logic Diagram<br>PRA Introduction & Event Trees<br>Fault Trees<br>Sample Return Capsule: Block Diagram, Logic, Schematics*<br>Back Up Material: ACS, Propulsion, Telecom Block Diagrams | Probabilistic-Risk-Assessment:<br>5131-05-209-SDU-PRA<br>5131-05-209-Att1-MLD<br>5131-05-209-Att2-EventTree<br>5131-05-209-Att3-FaultTrees<br>-<br>5131-05-209-Att5 |
| S6 | Project Decision Tables | Decision-Tables-<1, 2, 3> |
| S7 | Project Decision Tree | Decision-Tree |
| S8 | Project MIB Recommendations Response Plan | Gns-MIB-Project-Response |

* Not included in compact disk library due to proprietary content

| | **Project Area:** | **Flight Operations** |
|---|---|---|
| | File Location: | / Project-Documents / Flight / |
| REF | Document Name | File Name |
| F1 | Contingency Plan Safe Mode Recovery | CP-Safe-Mode-Recovery |
| F2 | Contingency Plan Stardust Propulsion System Anomaly | CP-Propulsion-Anomaly |
| F3 | Contingency Recovery Plan Loss of Signal, Anomalous Downlink | CP-Loss-of-Signal |
| F4 | Decommissioning Plan | Decommissioning-Plan |
| F5 | Deep Space Network Emergency Support | DSN-Spacecraft-Emergency |
| F6 | End of Days Operations Timeline | SRC-Release-OP-Timeline |
| F7 | Operational Interface Agreements<br>Entry State File<br>Spacecraft Trajectory File<br>Landing Location<br>STRATCOM State Vector<br>UTTR Look Angle File<br>Entry Trajectory File<br>Landing Ellipse<br>Conjunction Assessment Notice<br>Maneuver Design Initial Conditions | Operational-Interfaces:<br>301-Entry-State-File<br>302-Trajectory<br>303-Landing-Location<br>304-State-Vector<br>305-UTTR-Look-Angle<br>306-Entry-Trajectory<br>307-Landing-Ellipse<br>310-Conjunction-Assessment<br>311-Maneuver-Design-IC |
| F8 | Project Anomaly Reporting Plan | Anomaly-Reporting-Plan |
| F9 | Return Deep Space Network Summary Worksheet | Return-DSN-Summary |
| F10 | Spacecraft Mission Operations Procedure for SRC Release | SRC-Release-Ops-Proc |
| F11 | Spacecraft Mission Operations Procedure for SRC Release Redlines | SRC-Release-OP-Redlines |

| | **Project Area:** | **Test and Training** |
|---|---|---|
| | File Location: | / Project-Documents / Test-Training / |
| REF | Document Name | File Name |
| T1 | Flight Team Training Plan, Final for Earth Return Phase | Flight-Team-Training-Plan |
| T2 | Incompressible Test List | Incompressible-Test-List |
| T3 | SRC Release Sequence Test Plan | SRC-Release-Test-Plan |
| T4 | SRC Release Sequence Test Plan Flag Status Worksheet | SRC-Rel-Seq-Test-Flags-<1, 2> |
| T5 | SRC Release Test Program Status | SRC-Rel-Seq-Test-Plan-Sts |

| | **Project Area:** | **Planetary Protection** |
|---|---|---|
| | File Location: | / Project-Documents / Planetary-Protection / |
| REF | Document Name | File Name |
| P1 | Planetary Protection Classification Letter | Categorization-Letter |
| P2 | Planetary Protection Plan | Planetary-Protection-Plan |
| P3 | Planetary Protection Report, Part I, Pre-Launch Report | PP-Report1-PreLaunch |
| P4 | Planetary Protection Report, Part II, Post-Launch Report | PP-Report2-PostLaunch |
| P5 | Planetary Protection Report, Part III, End of Prime Mission Report | PP-Report3-EndofMsn |

## Project Documentation (Return Phase) (cont)

| | **Project Area:** | **Recovery Operations** |
|---|---|---|
| | File Location: | / Project-Documents / Recovery/ |
| REF | Document Name | File Name |
| R1 | Crew Training and Procedures Manual | Crew-Training-Manual |
| R2 | Helicopter Operations Safety Plan | Helo-Ops-Safety |
| R3 | Helicopter Recovery Operations Outline | Helo-Recovery-Ops-Outline |
| R4 | Helicopter Safety Manual | Helo-Safety-Manual |
| R5 | Mission Recovery Operations, Airworthiness and Flight Safety Review | ARC-AFSRB-Approval |
| R6 | Program Introduction Document The Stardust Project Addendum #2 | PID-Addendum2 |
| R7 | Recovered Flight Hardware Transport and Sample Canister Opening | Transportation-Procedure |
| R8 | Recovery Command System For Sample Return Capsule Recovery | Recovery-Cmd-System |
| R9 | Recovery Hazard Analysis Sample Return Capsule Operations | Recovery-Hazard-Analysis |
| R10 | Recovery Operations Graphical Timeline | Recovery-Timeline |
| R11 | Risk Coordination and Communications Notebook:<br>Table of Contents for Notebook<br>Stardust Return Main Message Points<br>RTQ: Stardust Sample Return, Entry, Descent, Landing and Rec…<br>Tribal Contacts and Liaisons<br>Nevada Tribes Contact Directory<br>Map of Indian Reservations and Colonies in Nevada<br>General Contacts (Telephone, email lists)<br>Points of Contact, Contingency Communications Team and Related<br>Earth Return Contingency Scripts<br>Earth Return Contingency Coordination Operations Plan<br>Mission Sample Return Risk Communication Plan<br>Contingency NASA Public Affairs Notification Tree | Risk-Comm-Notebook:<br>Table-of-Contents<br>Key-Messages<br>RTQs<br>Fema-Tribal<br>Tribal-Directory<br>Tribal-map<br>Impt-Phones<br>More-Contacts<br>Contingency-Scripts<br>NASA-Stardust-COP<br>Smpl-Ret-Risk-Comm-Plan<br>Table-C-1-CCOP |
| R12 | Sample Return Capsule Recovery Operations Plan | SRC-Rec-Ops-Plan |
| R13 | SRC Recovery Operations Procedure | SRC-Rec-Ops-Proc |
| R14 | SRC Recovery Operations Procedure Redlines #0 | SRC-Rec-OP-Redlines0 |
| R15 | SRC Recovery Operations Procedure Redlines #1 | SRC-Rec-OP-Redlines1 |
| R16 | SRC Recovery Operations Procedure Redlines #2 | SRC-Rec-OP-Redlines2 |
| R17 | SRC Recovery Operations Procedure Redlines #3 | SRC-Rec-OP-Redlines3 |
| R18 | Statement of Capability Revision 3 for STARDUST, Job Order Number.. | SOC-Revision3.pdf |
| R19 | USSTRATCOM Approval of Support* | - |
| R20 | USSTRATCOM Request for Support (FORM-1) | STRATCOM-Form1 |
| R21 | USSTRATCOM/JFCC SGS Functional Support Plan 8070-05 (U)* | - |

* Not included in compact disk library due to United States Strategic Command “For Official Use Only” status

| | **Project Area:** | **Curation** |
|---|---|---|
| | File Location: | / Project-Documents / Curation / |
| REF | Document Name | File Name |
| C1 | Recovery Inventory Procedure | Recovery-Inventory |
| C2 | Recovery: Handling of Loose Aerogel and Science Samples | Handling-of-Loose-Aerogel |
| C3 | Transfer of Space Exposed Hardware into Storage | Transfer-to-Storage |
| C4 | UTTR Clean Room Protocol | Clean-Room-Protocol |
| C5 | UTTR Spacecraft Processing Facility Contamination Control Monitor.. | Contamination-Control |

| | **Project Area:** | **Media** |
|---|---|---|
| | File Location: | / Project-Documents / Media / |
| REF | Document Name | File Name |
| M1 | Stardust Sample Return Press Kit | Sample-Return-Press-Kit |

## Project Reviews

| **Project Area:** | **Programmatics** |
|---|---|
| File Location: | / Project-Reviews |

| Document Name | File Name |
|---|---|
| Stardust Project Schedule, Revision 21, 5 Jan 2006 | Review-Schedule |

| **Review Name:** | **Stardust Programmatic Review** |
|---|---|
| Audience: | Discovery Program Office |
| Review Date: | 25 January 2005 |
| File Location: | /Project-Reviews/2005-01-25-NASA-Programmatic/ |

| Presentation Title | File Name |
|---|---|
| Stardust Programmatic Review | 1-Prog-Review |
| Stardust Cost Increases* | - |
| MIB Recommendations Response Plan | 3-Response-to-MIB |
| Reviews / Briefings / Plans / Responses … | 4-SDU-reviews |
| Review Plan Schedule | 5-SDU-schedule |
| Ancillary Products | File Name |
| Meeting Notes | Minutes-NASAProg |

* Not included in compact disc library due to proprietary content.

| **Review Name:** | **Stardust Project End of Mission Alternates Review** |
|---|---|
| Audience: | Navigation Advisory Group (Peers) |
| Review Date: | 04 March 2005 |
| File Location: | /Project-Reviews/2005-03-04-EOM-Peers/ |

| Presentation Title | File Name |
|---|---|
| Navigation Advisory Group (NAG) Review Stardust | 1-ChargetoBoard |
| Stardust Project End of Mission Alternates | 2-Sdu-Nag |
| Ancillary Products | File Name |
| Announcement of a Navigation Advisory Group (NAG) Review for Stardust | Announcement |
| Minutes of the Stardust NAG Review, 3/4/05 | Minutes-EOMNag |

| **Review Name:** | **Stardust Project End of Mission Alternates Review** |
|---|---|
| Audience: | Project Review Team |
| Review Date: | 15 March 2005 |
| File Location: | /Project-Reviews/2005-03-15-EOM-Alternates/ |

| Presentation Title | File Name |
|---|---|
| Introduction / Project Position | 1-3-Introduction |
| Stardust to Genesis Comparisons | 4-SDU-v-GNS |
| Daytime, Nighttime Spacecraft Operations | 5.1-Day-v-Night-Ops |
| Ground Impact Hazard Tracks | 5.2-Hazard-Tracks |
| STRATCOM and UTTR Considerations | 5.3-Non-NASA |
| SRC Entry & Margins | 5.4-SRC-EDL |
| Independent SRC Assessment | 5.5-Independent |
| Impacts to Nominal / Off-Nominal Recovery Operations | 5.6-Recovery |
| Backup Orbit / Follow-on Mission | 6.1-Backup-Orbit |
| Spacecraft Viability, Operations | 6.2-Backup-Ops |
| Safety and Mission Assurance Assessment | 7-MOA |
| Trade Study Summary | 8-Summary |
| Ancillary Products | File Name |
| Stardust End of Mission Alternates Review Team and Agenda | Agenda-EOMAlts |
| End of Mission Alternates Review Summary Report | Report-EOMAlts |

## Project Reviews (cont'd)

| **Review Name:** | **Stardust Project Mission Design and Navigation Return Peer Review** |
|---|---|
| Audience: | Peers |
| Review Date: | 14 April 2005 |
| File Location: | /Project-Reviews/2005-04-14-MDNAV/ |
| Presentation Title | File Name |
| Return Peer Review | 0-Cover |
| Introduction | 1-Introduction |
| Mission Overview | 3-Msn-Ovw |
| Earth Return Hazards | 4-ETESP-Hazards |
| SCT Flight Constraints | 5-SCT-Constraints |
| Calibration Plans | 6.1-CalPlans |
| Covariance Analysis for Earth Return and Atmospheric Entry | 6.2-OD |
| Entry, Descent, and Landing Trajectory Analysis Overview | 6.3-EDL |
| Maneuver Strategy | 6.4-MvrStrat |
| Delay, Safe Mode $\Delta V$, IIP Behavior | 6.5-Sensitivity-Hazards |
| Work to Go / Contingencies | 7-WrkToGo |
| Ancillary Products | File Name |
| Stardust Mission Design and Navigation Review Team and Agenda | Agenda-MDNAV |
| Earth Return Mission Design and Navigation Review Summary Report | Report-MDNAV |

| **Review Name:** | **Stardust Project Entry, Descent and Landing Peer Review** |
|---|---|
| Audience: | Peers (Analysts) |
| Review Date: | 02 June 2005 |
| File Location: | /Project-Reviews/2005-06-02-EDL-Peers/ |
| Presentation Title | File Name |
| Aerothermodynamics | 1-Aerothermal |
| PICA Analysis and Test (PAT) Project | 2.1-PICA |
| Thermal Protection System Analysis | 2.2-TPS |
| Stardust Trajectory Simulation Inputs | 3-Aerodatabase |
| Stardust SRC Aerodynamics | 4-Aerodynamics |
| Ancillary Products | File Name |
| Stardust EDL Peer Review Agenda | Agenda-EDLPeer |

| **Review Name:** | **Stardust Project Earth Targeting and Entry Safety Plan Review** |
|---|---|
| Audience: | Peers |
| Review Date: | 07 June 2005 |
| File Location: | /Project-Reviews/2005-06-07-ETESP/ |
| Presentation Title | File Name |
| Earth Targeting and Entry Safety Plan Review | 0-Cover |
| 1.0 Introduction | 1-Introduction |
| 2.1 Mission Overview | 2.1-Msn-Ovw |
| 2.2 ETESP Purpose, Scope, Process | 2.2-ETESP-Intro |
| 3.1 Breakup/burn up Cases | 3.1-BnB-Intro |
| 3.2 Spacecraft and SRC Components | 3.2-SC-SRC |
| 3.3.1 JPL Breakup & Burnup Analysis | 3.3.1-JPL-BnB |
| 3.3.2 Breakup and Burnup | 3.3.2-LM-BnB |
| 3.3.3 Breakup and Burnup: Aerospace Review | 3.3.3-AS-BnB |
| 3.3.4 Project Debris List | 3.3.4-Debris-List |
| 3.4.1 Landing Ellipse/IIP Behavior | 3.4.1-IIP-ellipse |
| 3.4.2 Earth LS & Probability Contours | 3.4.2-JPL-hazard |
| Hazard Analysis | 3.4.3-JSC-hazard |
| 3.4.4 Hazard/Contour Analysis: Aerospace Review | 3.4.4-AS-hazard |
| 3.5 Safety Analysis Conclusions | 3.5-Safety-Concl |
| 4.0 SRC Release and Divert Criteria | 4.0-Criteria |
| 4.4.1 Purple Button Risk | 4.4.1-Purple-Btn |
| 5.0 Work to Go | 5.0-Work-to-Go |
| Ancillary Products | File Name |
| Stardust Earth Targeting and Entry Safety Plan Review (Team and Agenda) | Agenda-ETESP |
| Stardust Earth Targeting and Entry Safety Plan Review Summary Report | Report-ETESP |

## Project Reviews (cont'd)

| **Review Name:** | **Stardust Project Entry, Descent and Landing Risk Review** |
|---|---|
| Audience: | Peers (System) |
| Review Date: | 16 June 2006 |
| File Location: | /Project-Reviews/2005-06-16-EDLSystem/ |
| Presentation Title | File Name |
| Entry, Descent and Landing Risk Review | 1-Overview-Summary |
| Simulation and Flight Dynamics | 2-Simulation |
| Risk Matrix Items – Avionics | 3-Gsw-testing |
| Aerothermodynamics | 4.1-Aerothermal |
| Thermal Protection System | 4-2-TPS |
| Parachute Recovery System (PRS) | 5-PRS |
| Ancillary Products | File Name |
| Stardust EDL Risk Review Agenda | Agenda-EDL |
| Entry Descent and Landing Risk Review Findings and Recommendations | Report-EDL |

| **Review Name:** | **Stardust Project Sample Return Capsule As-built Review** |
|---|---|
| Audience: | Peers |
| Review Date: | 17 June 2005 |
| File Location: | /Project-Reviews/2005-06-17-SRCSystem/ |
| Presentation Title | File Name |
| Sample Return Capsule As-built Review | 0-Cover |
| 1.0 Introduction | 1-Introduction |
| 2.1 Mission Overview | 2.1-Msn-Ovw |
| 2.2 SRC Overview | 2.2-SRC-Ovw |
| SRC Avionics Assembly | 3.1-SRC-Avionics |
| 3.2 G-switch Test Results | 3.2-Gsw-Tests |
| SRC Battery | 3.3-SRC-Battery |
| S/C to SRC Deadfacing | 3.4.1-SC-SRC-Deadface |
| 3.4b JPL Deadfacing Assessment | 3.4.2-JPL-Deadface |
| 3.5 Sep/Spin Mechanism | 3.5-Sep-Spin-Mech |
| 3.6 PRA | 3.6-PRA |
| 3.7 Reliability Analysis | 3.7-Reliability |
| 4.0 Summary: Risks, Mitigations, Work-to-Go | 4-Summary |
| Ancillary Products | File Name |
| STARDUST SRC As-built Review (Team and Agenda) | Agenda-As-Built |
| Mishap Investigation Board/Genesis Project Actions | Report-As-Built |

| **Review Name:** | **Stardust Project Recovery Operations Review** |
|---|---|
| Audience: | Peers |
| Review Date: | 21 June 2005 |
| File Location: | /Project-Reviews/2005-06-21-RecoveryOperations/ |
| Presentation Title | File Name |
| Recovery Operations Review-Morning Session | 1-Recovery-Review |
| Recovery Operations Review-Afternoon session | 2-Recovery-Review |
| Ancillary Products | File Name |
| SRC Recovery Operations Review (Agenda) | Agenda-Recovery |
| Recovery Operations Review Summary Report | Report-Recovery |
| SRC Recovery and Safety Review - Requests for Action (compilation) | RFAs-Recovery |
| Correlations of Board Finding to RFA | RFAtoReport-Map |

## Project Reviews (cont'd)

| **Review Name:** | **Stardust Project Sample Return Capsule Release and Fault Protection Review** |
|---|---|
| Audience: | Peers |
| Review Date: | 22 June 2005 |
| File Location: | /Project-Reviews/2005-06-22-SRCRelease/ |
| Presentation Title | File Name |
| 1.0 Introduction | 1-Introduction |
| 2.1 Mission To Date; 2.2 Release and Recovery Activities | 2.1n2-Msn-Ovw |
| 2.3 First Time and Critical Events; 2.4 Requirements | 2.3n4-FirstTime-Req |
| 3.0 Sequencing Background | 3-LM-Sequencing |
| 4.0 SRC Release Sequencing | 4-SRC-Release |
| 5.0 Fault Protection | 5.1-Fault-Protection |
| Stardust Return Fault Tree | 5.2-Fault-Tree |
| 6.0 STL Test Plan | 6-STL-Test-Plan |
| Ancillary Products | File Name |
| SRC Release Sequence and Fault Protection Review (Team and Agenda) | Agenda-Sequence |
| SRC Release and Fault Protection Review Final Report | Report-Sequence |
| Response to Review Board Comments | RFAres-Parameter-QA |

| **Review Name:** | **Stardust Project Flight Operations Review** |
|---|---|
| Audience: | Peers |
| Review Date: | 23 June 2005 |
| File Location: | /Project-Reviews/2005-06-23-FlightOperations/ |
| Presentation Title | File Name |
| 1.0 Overview | 1-Introduction |
| 2.0 Charge to Board | 2-Charge to Board |
| 3.0 Mission Overview | 3-Msn-Ovw |
| 4.0 Key Requirements | 4-Requirements |
| Pre-Launch Requirements V&V Matrix | 4.1-Backup |
| Navigation Plan | 5-Navigation |
| 6.0 SRC Release Sequencing | 6-SRC-Release-Divert |
| 7.0 ETESP Overview | 7-ETESP-Critieria |
| 8.0 Approach Spacecraft Support Plans | 8-SC-Support |
| 9.0 Flight Operations Support Plan | 9-FlightOps |
| 9.1 Detailed Operations Timeline | 9.1-Timeline |
| 10.0 Backup Orbit / Decommissioning | 10-BackupOrbit |
| 11.0 Test and Training Plan | 11-TestnTraining |
| 12.0 Mission Operations Assurance | 12-MOA |
| Ancillary Products | File Name |
| Flight Operations Review (Team and Agenda) | Agenda-FlightOps |
| Earth Return Flight Operations Review Summary Report | Report-FlightOps |

| **Review Name:** | **Stardust Project Risk, Certification and Implementation Review** |
|---|---|
| Audience: | Project Review Team |
| Review Date: | 19-20 July 2005 |
| File Location: | /Project-Reviews/2005-07-19-RiskReview/ |
| Presentation Title | File Name |
| Risk, Certification, Implementation Review | 0-Cover |
| Risk, Certification and Implementation Review | 0a-Final Agenda |
| 1. Introduction | 1-Introduction |
| 2. Overview | 2-Overview |
| 3a. New Project Baseline | 3.a-New Baseline |
| 3b. Project Interface Matrix | 3.b-Project-IF |
| SRC Avionics As-built Risk Report | 3.c-AsBuilt-Special |
| 3d.i Landing Site Selection Process: Recovery Team Selection | 3.d.i-Landing-Site |
| 3.d.ii Entry Targeting and Safety Validation | 3.d.ii-Target-Valid |
| 4. Navigation | 4-Navigation |
| 5. Spacecraft | 5-Spacecraft |
| 6.0 Fault Protection | 6-Fault-Protection |
| 7. SRC Release Sequence | 7-SRC-Release |
| 8.0 Mission Operations | 8-MissionOps |
| 9. Entry Targeting and Safety: Hazard Analysis | 9-ETESP-Hazards |
| 10. Entry Targeting and Safety: Decision Criteria | 10-ETESP-Criteria |
| 11. As-built SRC | 11-SRC-AsBuilt |

| | |
|---|---|
| EDL Risk Assessment | 12-EDL |
| 13. Recovery Operations | 13-Recovery |
| 14. Backup Orbit and Decommissioning | 14-Backup-Decom |
| 15.a. Test and Training: Flight Operations | 15.a-Flight-Training |
| 15.b. Test and Training: Recovery | 15.b-Recovery-Training |
| 15.c. Test and Training for RCS Support Organizations | 15.c-RCS-Training |
| 16. Residual Risk | 16-Residual-Risk |
| 17. Genesis MIB/FRB Response Summary | 17-MIB-FRB-sum |
| 18.a Project Schedules | 18.a-Project-Sch |
| 18.b.i. Mission/Project System Engineering | 18.b.i-SysEng-Impl |
| 18.b.ii Project Implementation: Team Schedules and Work Force: Navigation | 18.b.ii.Nav Impl |
| 18.b.iii Spacecraft Operations Implementation | 18.b.iii-SC-Impl |
| 18.b.iv. Mission Operations | 18.b.iv-MOS-Impl |
| 18.b.v. Project Implementation: Team Schedules and Work Force: Recovery … | 18.b.v-Rec-Impl |
| 18.b.vi-As Built SRC Work | 18.b.vi-AsBuilt-Impl |
| EDL Work to Go | 18.b.vii-EDL-Impl |
| 18.c.i Project Implementation: Project Funding Profile: LMSS Status | 18.c.i-LM-Funding |
| 18.c.ii Project Roll Up | 18.c.ii-Project-Funding |
| Risk, Certification, Implementation Review, Previous Review Reports and RFAs | A-Appendix |
| Board Recommendations to Stardust Mission | A0-Gns-MIB-to-SDU |
| Earth Return Mission Design and Navigation Review Summary Report | A1-Report-MDNAV |
| Earth Return Mission Design and Navigation Review RFAs | A1a-RFAs-MDNAV |
| Earth Targeting and Entry Safety Plan Review Summary Report | A2-Report-ETESP |
| Earth Targeting and Entry Safety Plan RFAs | A2a-RFAs-ETESP |
| Entry Descent and Landing Risk Review Findings and Recommendations | A3-Report-EDL |
| Entry Descent and Landing Risk Review RFAs | A3a-RFAs-EDL |
| Stardust SRC As-built Review Summary (email)/RFAs | A4-Report-AsBuilt |
| Stardust Recovery Operations Review Summary Report | A5-Report-Recovery |
| Recovery Review Disposition of RFAs | A5a-RFAs-Recovery |
| Sample Return Capsule Recovery Operations Plan Final Draft | A5b-SRC-Rec-Plan |
| SRC Release and Fault Protection Review Final Report | A6-Report-Sequence |
| SRC Release Sequence Review RFAs | A6a-RFAs-Sequence |
| Earth Return Flight Operations Review Summary Report | A7-Report-Flight Ops |
| Flight Operations Review RFAs | A7a-RFAs-Flight Ops |
| Ancillary Products | File Name |
| Risk, Certification and Implementation Review (Team and Agenda) | Agenda-Risk.r7 |
| Earth Return Risk, Certification and Implementation Review Summary Report | Report-Risk |
| Response to Stardust Risk Review Finding #6 | Response-Finding6 |
| Request for Action-Tina Beard | RFA1-Beard1 |
| Request for Action-Tina Beard | RFA2-Beard2 |
| Request for Action-Jenny Stein | RFA3-Stein1 |
| Request for Action-Jenny Stein | RFA4-Stein2 |
| Request for Action-Jenny Stein | RFA5-Stein3 |
| Request for Action-Dave Perkins (Savino) | RFA6-Savino1 |
| Response to Request for Action-Dave Perkins(Savino) | RFA6res-Risk |
| Request for Action (Mortelliti) | RFA7-Mortelliti1 |
| Request for Action (Mortelliti) | RFA8-Mortelliti2 |
| Request for Action (Mortelliti) | RFA9-Mortelliti3 |
| Request for Action (Mortelliti) | RFA10-Mortelliti4 |
| Request for Action (Mortelliti) | RFA11-Mortelliti5 |
| Response to Risk Review RFA #11 on CLT | RFA11res-Risk |
| Request for Action (Mortelliti) | RFA12-Mortelliti6 |
| Request for Action (Muirhead) | RFA13-Muirhead1 |

## Project Reviews (cont'd)

| **Review Name:** | **Stardust Project Residual Risk Review #1** |
|---|---|
| Audience: | Project Review Team (subset) |
| Review Date: | 23 August 2005 |
| File Location: | /Project-Reviews/2005-08-23-ResidualRisk1/ |

| Presentation Title | File Name |
|---|---|
| Residual Risk Review #1: EDL and SRC | 0-Cover |
| 1. Introduction | 1-Introduction |
| 2. Expanded Entry Flight Path Angle | 2-EFPA |
| EDL Risk Close Out | 3-EDL-Closeout |
| Sep/Spin Mechanism | 4-SSM |
| 5.0 Avionics Wrap Up | 5-Avionics |
| SRC Operating Voltage as SRC Internal Impedence Increases | 5.1-New-Chart |
| 6.0 SRC As-built Risk Close Out | 6-SRC-AsBuilt |
| 7. Appendix | 7-Appendix |
| Earth Return Risk, Certification, and Implementation Review Summary Report | 7.1-Report-Risk |
| Ancillary Products | File Name |
| Earth Return Residual Risk Review #1 Summary Report | Report-ResidRisk1 |

| **Review Name:** | **Stardust Project Residual Risk Review #2** |
|---|---|
| Audience: | Project Review Team (subset) |
| Review Date: | 21 September 2005 |
| File Location: | /Project-Reviews/2005-09-21-ResidualRisk2/ |

| Presentation Title | File Name |
|---|---|
| Residual Risk Review #2: Recovery and Flight Operations | 1-Residual-Risk-2 |
| Ancillary Products | File Name |
| Residual Risk Review 2 Agenda | Agenda-RRR2 |
| Earth Return Residual Risk Review #1 Summary Report | Report-RRR2 |
| Request for Action - Sevilla | RFA1-Sevilla1 |
| Request for Action - Sevilla | RFA2-Sevilla2 |
| Request for Action - Sevilla | RFA3-Sevilla3 |
| Request for Action - Brown/Mortelliti | RFA4-Mortelliti |

| **Review Name:** | **Stardust Project HQ Briefing** |
|---|---|
| Audience: | NASA HQ Science and Mission Directorate |
| Review Date: | 28 September 2005 |
| File Location: | /Project-Reviews/2005-09-28-HQ-Brief/ |

| Presentation Title | File Name |
|---|---|
| 1.0 Introduction | 1-Introduction |
| 2.0 Mission Goals and Science | 2-Msn-Sci-Goals |
| 3.0 Earth Approach and Landing | 3-Earth-Approach |
| 4.0 Assessment of Risk Posture | 4-Risk |
| 5.0 SRC Recovery | 5-Recovery |
| 6.0 Project Interactions | 6-Project |
| 7a End of Mission Alternates Review Summary Report | 7a-Report-EOM |
| 7b Earth Return Mission Design and Navigation Review Summary Report | 7b-Report-MDNAV |
| 7c Earth Targeting and Entry Safety Plan Review Summary Report | 7c-Report-ETESP |
| 7d Entry Descent and Landing Risk Review Findings and Recommendations | 7d-Report-EDL |
| 7e Mishap Investigation Board/Genesis Project Actions | 7e-Report-SRC-AsBuilt |
| 7f Recovery Operations Review Summary Report | 7f-Report-Recovery |
| 7g SRC Release and Fault Protection Review Final Report | 7g-Report-Sequence |
| 7h Earth Return Flight Operations Review Summary Report | 7h-Report-FlightOps |
| 7i Earth Return Risk, Certification and Implementation Review Summary Report | 7i-Report-Risk |
| 7j Earth Return Residual Risk Review #1 Summary Report | 7j-Report-RRR1 |
| Project Response Matrix to MIB Recommendations | 7k-MIB-Status |
| Project Schedule | 7l-Project-sch |
| Ancillary Products | File Name |
| Briefing Agenda / Discussion Topics | Agenda-SMD |

## Project Reviews (cont'd)

| **Review Name:** | **Stardust Project CAPTEM Board Review** |
|---|---|
| Audience: | CAPTEM Board (Curation and Analysis Planning Team for Extraterrestrial Materials) |
| Review Date: | 12 October 2005 |
| File Location: | /Project-Reviews/2005-10-12-CAPTEM/ |
| Presentation Title | File Name |
| Stardust Status Preliminary Examination | 1-PET-Status |
| Major Stardust PE Operations | 2-PE-Operation |
| Preliminary Examination-Sample Requests | 3-PE-Request |
| Ancillary Products | File Name |
| Stardust Status Preliminary Examination | Minutes-Apdx10 |
| Major Stardust PE Operations | Minutes-Apdx11 |
| A collection of tools for the Stardust Sample Prep Toolbox | Minutes-Apdx12 |
| Documentation of Stardust Interstellar Dust Collector | Minutes-Apdx13 |
| Stardust Sample Allocation (after preliminary examination) | Minutes-Apdx14 |
| Captem Minutes-B, Minutes of the Thirtieth Meeting of the CAPTEM | Minutes-Captem |
| Response to CAPTEM Finding and Recommendations regarding Stardust … | Recovery-Res-to-CAPTEM |

| **Review Name:** | **Stardust Project Residual Risk Review #3** |
|---|---|
| Audience: | Project Review Team (subset) |
| Review Date: | 13 October 2005 |
| File Location: | /Project-Reviews/2005-10-13-ResidualRisk3/ |
| Presentation Title | File Name |
| Residual Risk Review #3 | 0-Cover |
| Residual Risk Review #3 Agenda | 0a-Agenda |
| 1.0 Introduction | 1-Introduction |
| 2a. Maneuver Certification Rationale | 2a-Mnvr-Cert-Rationale |
| 2b. Maneuver Certification Process | 2b-Mnvr-Cert-Process |
| 2.0.c Maneuver Certification | 2c1-ACS-MainBurn |
| Maneuver Certification ACS Small Forces Analysis | 2c2-ACS-Turns |
| In-Flight Calibration of Expected Maneuver Performance | 2c3-NAV-Calibrations |
| 2.0 d. Resulting Navigation Performance | 2d-NAV-Performance |
| 3. Moon and Star Camera FOV | 3-Moon-Bright-Body |
| 4. Decision Tree-Introduction | 4a-Dec-Tree-Intro |
| Stardust Project Decision Tree | 4b-Decision-Tree |
| Stardust Flight Operations Key Decisions | 4c1-DecisionTables |
| Stardust Recovery Operations Key Decisions | 4c2-DecisionTables |
| Stardust Recovery Command System Operations Key Decisions | 4c3-DecisionTables |
| 5.0 Project Staffing Plan | 5-Staffing-Plan |
| Navigation Staffing Schedule | 5a-NAV-Staffing |
| Spacecraft Staffing Schedule | 5b-SCT-Staffing |
| 6.0 Miscellaneous Recovery Findings | 6-Recovery-topics |
| 7.0 Independent Safety Review Team (IRT) | 7-IRT |
| Ancillary Products | File Name |
| Residual Risk Review #3 (Team and Agenda) | Agenda-RRR3 |
| Earth Return Residual Risk Review #3 Summary Report | Report-RRR3 |

| **Review Name:** | **Stardust Project Safety Review Board** |
|---|---|
| Audience: | UTTR Safety and Command Personnel |
| Review Date: | 19 October 2005 |
| File Location: | /Project-Reviews/2005-10-19-SafetyReviewBoard/ |
| Presentation Title | File Name |
| Safety Review Board | 1-SRB-Briefing |
| Ancillary Products | File Name |
| Utah Test and Training Range Mission Safety Review | 2-SRB-Approval |

## Project Reviews (cont'd)

| **Review Name:** | **Stardust Project Ground Data Systems Readiness Review** |
|---|---|
| Audience: | Peers |
| Review Date: | 17 November 2005 |
| File Location: | /Project-Reviews/2005-11-17-GDSReadiness/ |
| Presentation Title | File Name |
| SRC Return | 1-MGSS-Readiness-Review |
| Ancillary Products | File Name |
| GDS Readiness Review Minutes | Minutes-GDSRR |

| **Review Name:** | **Stardust Project Navigation Readiness Review** |
|---|---|
| Audience: | Navigation Advisory Group (Peers) |
| Review Date: | 18 November 2005 |
| File Location: | /Project-Reviews/2005-11-18-NAVReadiness/ |
| Presentation Title | File Name |
| Earth Return Readiness Review for Navigation Advisory Group (NAG) | 0-Cover |
| 1. Introduction | 1-Introduction |
| 2. Mission Background | 2-Mission |
| Stardust Project Decision Tree | 2a-DecisionTree |
| Stardust Flight Operations Key Decisions | 2b1-DecisionTables |
| Stardust Recovery Operations Key Decisions | 2b2-DecisionTables |
| 3.a. Deadband Walk Calibrations | 3a-DBW-Cal |
| 3.b. Entry Maneuver Calibrations | 3b-EMD-Cal |
| 3.c. Limit-Cycle Calibrations | 3c-LC-Cal |
| 4. TCM Strategy | 4-TCM-Strategy |
| 5. OD Strategy | 5-OD-Strategy |
| OD Process | 6a-OD-Process |
| Entry, Descent, and Landing | 6b1-EDL-Process |
| 6b (part 2) Earth LS | 6b2-EarthLS-Process |
| 6c(i) TCM Procedures | 6ci-FullDesign-Proc |
| 6.c.ii Fixed Attitude (TCM19/TCM19-a) | 6cii-FixedDirection-Proc |
| Design of Pre-planned Maneuvers | 6c-PrePlanned-Maneuvers |
| 6.d.i.-SRC Release-Enable (Green Button OD & EDL Contributions) | 6di-SRC-Release-Enable |
| 6.(d)ii. Nav Evaluation for SRC Release Disable (Red Button) | 6dii-SRC-Release-Disable |
| 6.d.iii SRC Release Verification | 6diii-SRC-Rel-Verification |
| 6e. JPL-UTTR/STRATCOM Interface | 6e-UTTR-Stratcom |
| 7a. Facilities, Workstations, Communications | 7a-Facilities |
| Software Versions and Testing | 7b-Software |
| 7c. Operational Interface Agreements | 7c-OIAs |
| 7d. Personnel and Staffing Schedule | 7d-Staffing |
| Navigation Staffing Schedule | 7d1-Staffing-Plan |
| 8. Test Results/Plans and Open Issues | 8-TestnTraining |
| Ancillary Products | File Name |
| Update NAG Agenda | Agenda-NAVReadiness |
| Stardust NAG and Readiness Review | Board-NAVReadiness |
| Summary Report: Stardust Earth Return Readiness Review for Navigation … | Report-NAVReadiness |
| Regression Test of MarsLSv3.0 for Stardust Operations | RFAres-EarthLS |
| Review of GRAM Atmosphere for Stardust | RFAres-EDL-Atmos-rvw |
| Stardust Simulation Parameter Review | RFAres-EDL-Param-rvw |

| **Review Name:** | **Stardust Project Utah Test and Training Range Readiness** |
|---|---|
| Audience: | Peers |
| Review Date: | 30 November 2005 |
| File Location: | /Project-Reviews/2005-11-30-UTTRReadiness/ |
| Presentation Title | File Name |
| <none – verbal telecon> | |
| Ancillary Products | File Name |
| UTTR Mission Readiness Review | Agenda-UTTRReadiness |

## Project Reviews (cont'd)

| **Review Name:** | **Stardust Project Deep Space Network Readiness Review** |
|---|---|
| Audience: | DSN Management Team |
| Review Date: | 02 December 2005 |
| File Location: | /Project-Reviews/2005-12-02-DSNReadiness/ |

| Presentation Title | File Name |
|---|---|
| Sample Return Capsule Mission Event Readiness Review | 1-Introduction |
| Stardust Navigation | 2-Navigation |
| SFOC Facility | 3-SFOC-Facility |
| AMMOS Readiness | 4-Ammos |
| Network Infrastructure | 5-Network |
| DSN Operations | 6-DSN-Net-Ops |
| Critical Event Planning | 7-Planning |
| TMS Manager's Comments | 8-Mgr-Assessment |
| **Ancillary Products** | **File Name** |
| Stardust DSMS Mission Event Readiness Review MERR | Agenda-MERR |
| DSMS Review Report | Report-MERR |
| Ranging Configurations | RFA-Closure |
| Stardust Uplink MSTA Test Results | RFA-ECC-UL |

| **Review Name:** | **Stardust Project Critical Events Readiness Review** |
|---|---|
| Audience: | Project Review Team |
| Review Date: | 06 December 2005 |
| File Location: | /Project-Reviews/2005-12-06-CE-Readiness/ |

| Presentation Title | File Name |
|---|---|
| Critical Events Readiness Review | 0-Cover |
| 1. Project Overview | 1-Overview |
| 2. Flight Operations Plan | 2a-FlightOps |
| Stardust End of Days-Rev 15 | 2a-Timeline |
| 2b. Flight Team Training | 2b-FlightTeamTnT |
| 3a. Landing Ellipse Crosstrack Strategies | 3a-Landing-Ellipse |
| 3b.Yellow Divot and Site Selection Assessment Update | 3b-YellowDivot |
| 3c. Changes to the Recovery Plan | 3c-Recovery |
| 4a. SRC Release/Divert Critical Sequence | 4a-Sequence |
| 4b. Sequence V&V | 4b-Sequence-VnV |
| 5. Recovery Operations Plan | 5-Recovery Ops |
| 6a. Independent Recovery Team (IRT) | 6a-IRT |
| (SRC Structure Thermal Response Model Discrepancy) | 7-SRC-Structure |
| 7a. Risk Process and Results | 7a-Risk Process |
| 7b. Residual Risk Report (Mission Operations Assurance) | 7b-MOA |
| EDL Reviews RFA Closure Matrix | 7b1-EDL |
| 7c. Residual Risk Report (System Safety) | 7c-Safety |
| 8a. Spacecraft Readiness | 8a-SC-Readiness |
| 8b. Navigation Readiness Report | 8b-NAV-Readiness |
| NAV Reviews RFA Closure Matrix | 8b1-NAV-Update |
| 7c [sic] Readiness Report: Deep Space Network | 8c-DSN-Readiness |
| 8d. Mission Operations (including GDS) | 8d-MOS-Readiness |
| 8e. Readiness Reports - Recovery | 8e-Recovery-Readiness |
| 8f. Recovery Command System | 8f-RCS-Readiness |
| USSTRATCOM Readiness | 8g-USSTRATCOM-Readiness |
| 8.h Key Staff & Decision Makers | 8h-KeyDeciders-Plan |
| 10. [sic] Media Relations | 9-Media-Readiness |
| **Ancillary Products** | **File Name** |
| Critical Events Readiness Review (Team and Agenda) | Agenda-CERR |
| Earth Return Critical Event Readiness Review Summary Report | Report-CERR |
| Request for Action-D. Kontinos | RFA-Kontinos |

## Project Reviews (cont'd)

| **Review Name:** | **Stardust Project Safety and Mission Assurance Readiness Review** |
|---|---|
| Audience: | NASA Office of Safety and Mission Assurance, Chief Engineer |
| Review Date: | 9 December 2005 |
| File Location: | /Project-Reviews/2005-12-09-SMA-Readiness/ |

| Presentation Title | File Name |
|---|---|
| Stardust Earth Return Safety and Mission Assurance Readiness Review | 1-Introduction |
| Stardust Assurance Process Map | 1a-AP-Map |
| Safety & Mission Assurance Readiness Assessment (SMARR): Earth Return | 2a-MOA |
| Star Camera ISA (Z87821) | 2b-SCAM-Outage |
| 9. [sic] Entry Targeting and Safety: Hazard Analysis | 2c-ETESP-Hazards |
| 2. [sic] Flight Operations Plan | 2d-FlightOps |
| Stardust Safety and Mission Assurance Readiness Review (SMARR): Safety … | 3-Recovery-Safety |
| Readiness Poll | 4-Readiness-Poll |
| Ancillary Products | File Name |
| Stardust Safety and Mission Assurance Readiness Review (SMARR)-Readi ... | Poll-SMARR |
| Safety and Mission Assurance Readiness Review (SMARR) Process | Process-SMARR |

| **Review Name:** | **Stardust Project JPL Governing Council Readiness Review** |
|---|---|
| Audience: | JPL Governing Council |
| Review Date: | 15 December 2005 |
| File Location: | /Project-Reviews/2005-12-15-JPL-GoverningCouncil/ |

| Presentation Title | File Name |
|---|---|
| 1. Introduction | 1-Introduction |
| 2. Science | 2-Science |
| 3. Mission Preparations | 3-Mission |
| Stardust Project Decision Tree | 3a-DecisionTree |
| Stardust Flight Operations Key Decisions | 3b1-DecisionTable |
| TCM-19ab Build Map | 3b2-DecisionTable |
| Stardust Recovery Operations Key Decisions | 3b3-DecisionTable |
| 4. Readiness Report Deep Space Network | 4-DSMS |
| 5. Spacecraft Preparations | 5-Spacecraft |
| 6. Recovery Preparations | 6-Recovery |
| 7. Mission Operations Assurance Assessment | 7-MOA |
| 8. Risk Management Process | 8-Risk |
| 9. Genesis MIB Assessment | 9-MIB |
| 10. Safety Assessment | 10-Safety |
| 11. Project Assessment | 11-Project |
| Ancillary Products | File Name |
| GPMC (Scope and Agenda) | Agenda-GPMC |
| Stardust Project Post CERR (Earth Return) GPMC JPL Director GPMC | Report-GPMC |

| **Review Name:** | **Stardust Project LMSS President's Readiness Review** |
|---|---|
| Audience: | LMSS President |
| Review Date: | 19 December 2005 |
| File Location: | /Project-Reviews/2005-12-19-LMSS-Presidents/ |

| Presentation Title | File Name |
|---|---|
| President's Mission Success Review | 1-LM-Presidents |
| Ancillary Products | File Name |
| | |

## Project Reviews (cont'd)

| **Review Name:** | **Stardust Project HQ Mission Readiness Briefing** |
|---|---|
| Audience: | NASA HQ Science and Mission Directorate |
| Review Date: | 21 December 2005 |
| File Location: | /Project-Reviews/2005-12-21-HQ-MissionReadiness/ |

| Presentation Title | File Name |
|---|---|
| 1. Introduction | 1-Introduction |
| 2. Science | 2-Science |
| 3. Mission Status | 3-Mission |
| Stardust Project Decision Tree | 3a-DecisionTree |
| Stardust Flight Operations Key Decisions | 3b1-DecisionTable |
| TCM-19ab Build Map | 3b2-DecisionTable |
| Stardust Recovery Operations Key Decisions | 3b3-DecisionTable |
| 4. Spacecraft Status | 4-Spacecraft |
| 5. Recovery Status | 5-Recovery |
| 6. Risk Management Process | 6-Risk |
| 7. Genesis MIB Assessment | 7-MIB |
| 8. Project Status | 8-Project |
| Ancillary Products | File Name |
| NASA SMD PMC for STARDUST (Agenda) | Agenda-MRB |