

Stardust Blazes MOA Trail

Grant B. Faris¹ and Larry W. Bryant²
Jet Propulsion Laboratory/California Institute of Technology
Pasadena, CA 91109

[Abstract] **Mission Operations Assurance (MOA) started at the Jet Propulsion Laboratory (JPL) with the Magellan and Galileo missions of the late 80's. It continued to develop and received a significant impetus with the failures of two successive missions to Mars in the late 90's. MOA continued to evolve with each successive project at JPL achieving its current maturity with the Stardust sample return to Earth.**

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 the NASA Headquarters counterparts. 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 would provide invaluable insight to the Project regarding evolving institutional requirements and expectations in preparation for the Sample Return Capsule (SRC) return and recovery.

The discussion below describes the participation of the Stardust mission operations assurance manager in the preparation effort for the SRC return. In general the mission operations assurance effort was conducted in parallel to the detailed preparation by the flight team, providing the independent perspective to project and institutional management. The results achieved provide the basis for the continued growth of the MOA discipline at JPL and throughout the Space Operations Community.

I. Historical Background

When the Challenger exploded in 1986, one of the immediate results at JPL was the delay in the launch of the Galileo spacecraft to Jupiter. The ensuing accident investigation made it abundantly clear that there were residual risks from development activities that could affect flight operations. Consequently, JPL made the decision to extend the normal Mission Assurance function into flight operations to independently identify and assess residual development risks as well as perform an ongoing assessment of risk throughout the operational mission. Thus as Magellan (which was now scheduled to launch on the shuttle ahead of Galileo) and Galileo prepared for their interplanetary launches from the space shuttle, the concept of Mission Operations Assurance was born at JPL.

¹ Chief Mission Operations Assurance Manager, 5150-Mission Assurance Management Office, 4800 Oak Grove Drive, MS 264-235

² Mission Operations Assurance Manager for MRO, MER, and WISE, 5150-Mission Assurance Management Office, 4800 Oak Grove Drive, MS 264-535, Senior

Mission Operations Assurance evolved over the next decade at JPL. With the failure of the Mars Climate Orbiter in 1999, the subsequent failure review board made specific findings and recommendations in the area of mission assurance. These were captured in the NASA Public Lessons Learned.¹

1. Although a Mission Assurance Manager (MAM) was assigned to Mars Climate Orbiter (MCO) during project development, there was no independent mission assurance function established for the work performed at JPL following launch.
2. Discrepancies between the delta-Vs expected by the Navigation Team and those produced by the Angular Momentum Desaturation (AMD) file from the Spacecraft Team were observed during mission operations. However, no Incident/Surprise/Anomaly (ISA) or Problem/Failure Report (P/FR) was written on this issue.

The two associated recommendations were implemented in JPL's institutional Flight Project Practices.

1. Revise JPL mission assurance policies and procedures to require an independent Mission Assurance representative during the operational phase of every flight project. This individual should become familiar with and be integrated into the project during the latter phases of development, and possess independent responsibility to verify compliance with design and operational requirements.
2. Require all flight projects to report and track post-launch anomalies on ISAs. Project management should rigidly enforce this requirement and maintain a disciplined disposition, tracking, and resolution process.

JPL continued to mature and improve its MOA process with each succeeding mission to Mars, Saturn, the Sun, comets, and even returning samples to Earth. It was the return to Earth that really gave MOA the final impetus needed to formalize and codify the rigor required to provide an independent assessment to contribute to the mitigation of risk as the Stardust Science Return Capsule (SRC) came blazing back to Earth.

II. Preparing to Return

The independent review and assessment of the Stardust Project's risk posture was performed to facilitate the mitigation of flight operational risks to the sample return operations. This assessment would ultimately be 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 is typically done in preparation for launch. However, the Stardust Earth return was equally critical due to the safety implications of bringing a sample return capsule over the continental United States and 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 (P/FRs), 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. One lesson going forward, especially for long duration missions is that 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's (ISAs) and operational waivers with implications to Earth return.

To characterize compliance with institutional standards, the Stardust's Earth return plans were compared with JPL's Flight Project Practices (FPPs) and Design Principles (DPs). 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 would include validation testing in the spacecraft test laboratory along with flight team and ground recovery team operational exercises. An ITL is 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 FPP non-compliances in the area of project organization with negligible residual risk for Earth return and 14 DP 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 (ORTs) 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 testing 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 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 operational readiness test revealed a situation in which an incorrectly set criteria could cause an unnecessary wave off and place the SRC into a backup orbit returning four years later. The result of this vulnerability was the establishment of the Anomaly Panel and re-examination of the decision criteria construct.

In addition to active participation in the training exercises, mission operations assurance worked hand-in-hand with the 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.

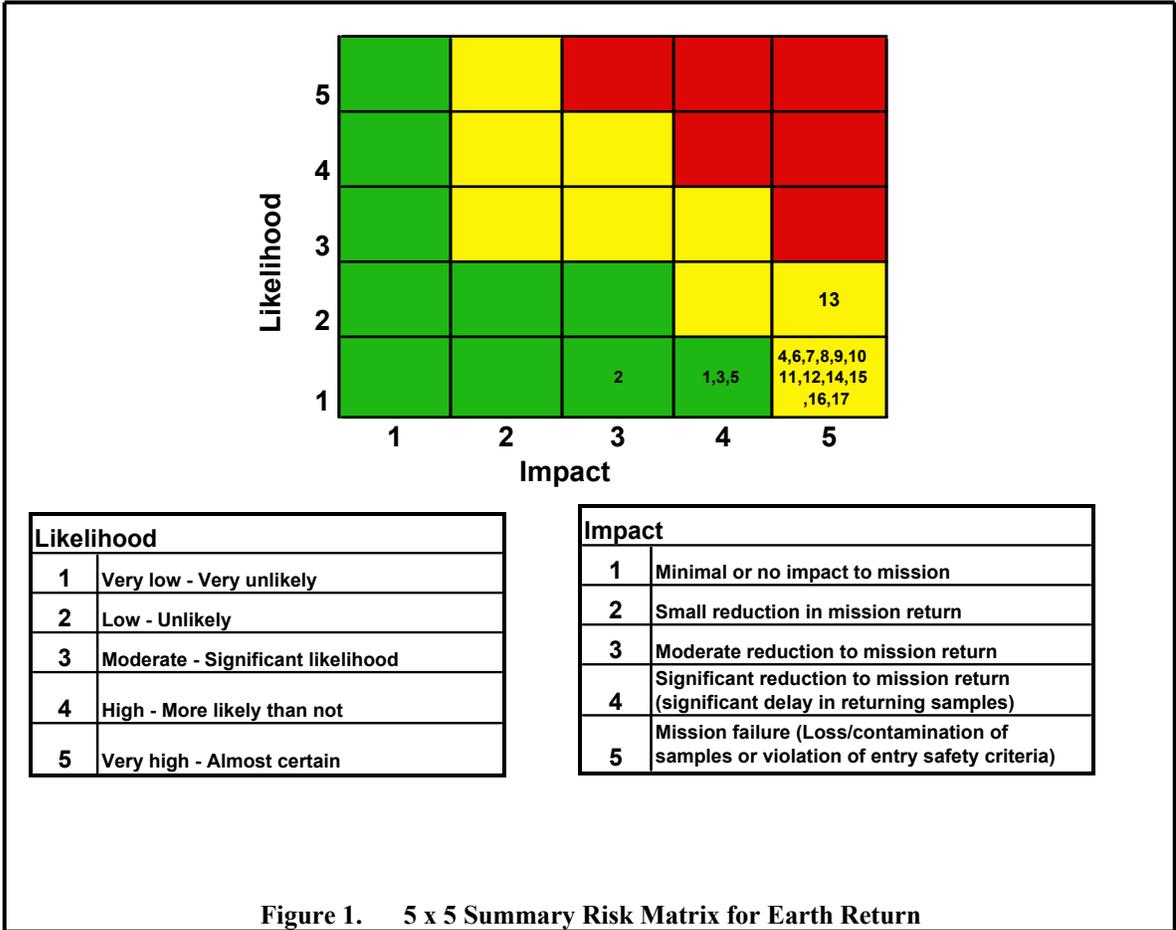
III. Assessing the Risk

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 by the specifics of the Stardust Project, are described in the following sections.

A. 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. For example, the impact rating of 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. The significant reduction in mission return (impact = 4) rating was redefined as significant delay in returning samples due to diverting to the backup orbit.

Figure 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 represent 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. This type of ratio is often observed for critical events due to the nature of the activity.



B. Residual Risk List and Example Earth Return Residual Risk Description Summary

The residual risk list is 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 is continually reviewed and modified throughout the life of a flight project. The residual risk list shown in Figure 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 are somewhat subjective or qualitative, and the actual numbers are not as important as the discussion of each residual risk and its communication through the management chain. Figure 3 is an example of a detailed residual risk description that includes the objective rationale supporting the particular selection of impact and likelihood ranking, but more importantly serves as the information conduit. Residual risk 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 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 3. Earth Return Residual Risk Description

C. 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 Office of Safety and Mission Success and accepted as the Project position going into the review.

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.

<u>Risk Drivers</u>	<u>Nighttime</u>		<u>Daytime</u>	
	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 4. Risk Balance Trade – Nighttime versus Daytime Entry

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.

D. 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, 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 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.		P/SE/MS/SE	Contr.	MM/MS/SM	MA/MS/SS	PM/PT	OCE	OS/MS	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, idiosyncrases, 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 Cat 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 MB issues have been addressed and dispositioned.	x	x	x	x	x		x		Letter from MB chair states all items were addressed.
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 5. Stardust CoCER Compliance Matrix

IV. Stardust Results 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.

V. Current Position and Direction

Following the recommendations of the Mars 98 reports, a list of 13 mission assurance type activities was assembled. Each was accompanied by a set of roles for systems engineering and for mission operations assurance. These activities and roles provided guidance for project mission operations assurance, but did not provide a structured plan for implementation of an effective program. Stardust's effort provided a practical template for the implementation of an effective and complete Mission Operations Assurance Program. The challenge was to take advantage of the guidelines along with the Stardust experience. By melding the two we hoped to develop a plan template and propagate it throughout JPL's mission operations to promote consistent implementation across projects.

The foundation of our plan was the requirements for Mission Operations Assurance contained in JPL's Flight Project Practices. These focused in three areas of projects having a Mission Operations Assurance Manager, developing a Mission Operations Assurance Plan (MOAP), and obtaining an independent assessment of the project's operational readiness. Building on this foundation and keeping in mind other

relevant requirements, such as those relating to problem reporting and risk management, we identified a set of requirements for a mission operations assurance program.

- 1) MOA shall independently assess project risks throughout mission operations.
- 2) MOA shall independently assess the project's operational readiness to support nominal and contingency mission scenarios.
- 3) MOA shall implement the project's problem/failure reporting system (P/FRS) to comply with JPL's Anomaly Resolution Standard (current version).
- 4) MOA shall provide training on problem reporting for the flight team.

With requirements as a basis, the Stardust experience, and a revised Anomaly Resolution Standard, we were ready to develop a template for use throughout JPL's flight projects for their implementation plan for mission operations assurance.²

The template which resulted from this effort was completed in August of 2009 and was first used by the Wide-field Infrared Survey Explorer (WISE) as the basis for the project MOAP. WISE is a single instrument in a sun synchronous earth orbit. Its basic function is to map the entire sky in four infrared bands. The relative simplicity and primarily in-house (JPL) nature of the operational mission allowed the MOAP template to be tailored for WISE quickly and easily. The major focus for tailoring was the process of documenting incidents, surprises, and anomalies occurring during operations. Because WISE was the first project to use JPL's new institutional Problem Reporting System (PRS) for Incident, Surprise, Anomaly (ISA) reports, it was important to be very clear in describing use of the new system over the legacy system to minimize confusion for the flight team during this rollout. The second project to make use of the template, Juno, faced a different set of tailoring issues.

The Juno project wanted to establish requirements for MOA support, particularly problem reporting, for all project participants, including contractors and academic institutions. This meant adding a section for project level requirements related to MOA and incorporating material from institutional documents that are normally not available to project participants outside of JPL. Another aspect to be addressed was the fact that Juno is transitioning from JPL's legacy ISA system to the ISA element of PRS. Consequently, additional information was needed to insure project members had adequate guidance in the use of both systems to make the transition as seamless as possible. Even with the increased need for project specific tailoring of the MOAP template for Juno as opposed to WISE, the Preliminary version was completed, reviewed, approved and signed by the project well over a month prior to the required delivery date of the Juno Systems Integration Review (SIR). Efforts are also on-going to disseminate the MOAP template to the space operations community at JPL and other locations to provide projects with a solid framework for an effective program to contribute to their mission success.

One area at JPL is through the Project Support Office which has a database of templates and samples of documents for projects to draw from. This capability to have reusable plans avoids re-inventing the wheel while still providing flexibility to adapt to project specific needs. A second area is the AIAA Space Operations and Support Technical Committee "Space Operations Best Practices" document. A version of the template has been cleared for unconditional release and provided to the committee as an input for a new section of the document. We hope in this way to extend the mission operations assurance concept throughout the space operations community and give each project a roadmap for enhancing their assurance of a successful mission.

References

¹ Oberhettinger, D., "Mission Assurance During Mars Climate Orbiter Operations (1999)," NASA Public Lessons Learned Entry: 0886, Apr 2000

² Bryant, L., "Mission Operations Assurance Plan Template," JPL D-60499, Aug 2009