[Abstract] The Mission Operations Assurance (MOA) discipline actively participates as a project member to achieve their common objective of full mission success while also providing an independent risk assessment to the Project Manager and Office of Safety and Mission Success staff. The cornerstone element of MOA is the independent assessment of the risks the project faces in executing its mission. Especially as the project approaches critical mission events, it becomes imperative to clearly identify and assess the risks the project faces. Quite often there are competing options for the project to select from in deciding how to execute the event. An example includes choices between proven but aging hardware components and unused but unproven components. Timing of the event with respect to visual or telecommunications visibility can be a consideration in the case of Earth reentry or hazardous maneuver events. It is in such situations that MOA is called upon for a risk balance assessment or risk trade study to support their recommendation to the Project Manager for a specific option to select. In the following paragraphs we consider two such assessments, one for the Stardust capsule Earth return and the other for the choice of telecommunications system configuration for the EPOXI flyby of the comet Hartley 2. We discuss the development of the trade space for each project’s scenario and characterize the risks of each possible option. The risk characterization we consider includes a determination of the severity or consequence of each risk if realized and the likelihood of its occurrence. We then examine the assessment process to arrive at a MOA recommendation. Finally we review each flight project’s decision process and the outcome of their decisions.

I. Introduction

As Hamlet has mused through the centuries, "To be, or not to be, that is the question." As intrepid space explorers age in their extended missions, it's a question projects must often revisit. Even spacecraft well within their design lives must often re-examine previous decisions to decide if they may stand or must be put aside. We will take the youthful case first and examine a decision made by the Stardust mission and how it had to be reexamined. This first case deals with the re-entry and Earth landing of a Sample Return Capsule (SRC) filled with aerogel which held particulate samples of the Comet Wild 2. The landing was planned for a military test range in the middle of Utah rather than the broad ocean area used for manned re-entry as well as tests of re-entry vehicles. This implies the possible overflight of and landing near populated areas. Needless to say, Human Safety is a major concern for this sort of plan. As the return grew near, the human safety concern prompted a reexamination of the initial decision for the atmospheric reentry to occur at night. The second example we will consider is the re-cycled Deep Impact flyby spacecraft well into its extended mission named EPOXI.

Deep Impact was a two part spacecraft, one part flyby system and one part impactor system. On July 4, 2005, the impactor was released from the flyby and impacted the nucleus of comet Tempel 1. Part of the follow-on extended mission was to do a close flyby of the comet Hartley 2. The thrust of this encounter was to image the core of the comet at close range and return the images to Earth shortly thereafter. Key in this was the playback of images which required a functioning telecom system. During the extended mission, EPOXI had seen some anomalous behavior of its telecom system which prompted the examination of several options for switching between the low

1 Mission Operations Assurance Manager for Juno, MRO, MER, and WISE, 5150-Mission Assurance Management Office, 4800 Oak Grove Drive, MS 264-767, Senior.
2 Chief Mission Operations Assurance Manager, 5150-Mission Assurance Management Office, 4800 Oak Grove Drive, MS 264-235.

The research described in this paper was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.
gain and high gain antennas during the encounter time frame. The focus of our review in both instances is the risk balance or risk trades between the options available to the project with the objective of picking the option that maximizes the likelihood of mission success.

We consider mission success as meeting level 1 requirements within cost and schedule with acceptable risk and doing it safely. Risk is the likelihood of an undesirable event/outcome occurring AND the severity of the consequences of the occurrence. Likelihood is characterized by two major parameters – conditions and window of vulnerability. Consequence is characterized as either mission impact or implementation impact, and by the set of possible outcomes should the risk item occur. Experience indicates that risks are derived from several root causes:

- Unsettled definition of mission Level 1 requirements, priorities and full/minimum success criteria
- Incomplete understanding of the driving mission/system requirements, including the impact of mission time-critical activities
- Lack of sufficient margins (technical and programmatic)
- Unsubstantiated assumptions (which are usually optimistic)
- Incomplete identification of key risks and mitigation options
- Unsubstantiated optimism of the capabilities of the project team and/or its contractors/partners
- Unknown Unknowns

The last cause, unknown unknowns, is clearly the most insidious because of the inherent uncertainty of not knowing what you don’t know. The risk can never be driven to zero, but the objective is to have a level of residual risk that is acceptable (a subjective term) when compared to the return of a successful mission. Deep space missions have a set of characteristics that contribute to mission risk. Key among these are the following:

- Challenging One-of-a-kind
- Long Life
- Complex Missions and Payloads
- Extreme Environments (e.g. Mars surface, space and planetary radiation)
- Time-critical Mission Activities
- Long Communication Distances
- Cost and Schedule Constrained

As we examine the cases below, we will see a number of these characteristics playing a role in the risk drivers we consider.

### II. Risk Balance Background

Unique characteristics of the Stardust mission presented management with a very challenging risk trade space. The return of the Sample Return Capsule (SRC) for a landing at the Utah Test Range meant that populated areas were being overflown by an object reentering through Earth’s atmosphere from deep space. Other objects, such as manned capsules, landed in a Broad Ocean Area (BOA) and their return path kept them safely away from populated areas. While Genesis had performed a similar return, there were time of day options for the Stardust return that dictated a careful study of the available risk trades.

Unlike Genesis, whose planned mid-air helicopter recovery dictated a daytime return, Stardust initially planned a nighttime return to Earth. As the return date approached, concerns over night time operations and recovery crew safety prompted a request for reexamination of the risks associated with return time options. The intuitive perception was that a return at night would pose more risk of human injury than a daytime return. Since human safety is a paramount concern in space exploration, it was prudent for the Mission Operations Assurance Manager (MOAM) to reassess the risks of both options and provide an independent risk-balance trade recommendation.

The general approach to provide an independent Mission Assurance assessment of the Project’s options for dealing with an approaching condition/event considers the risk to the spacecraft and to the spacecraft plus, in some cases, to the general population and/or the environment. The initial step is to identify the risk items through a review of key areas such as:

- Spacecraft safing history, especially during critical times
- Maintaining redundant/backup capability
- Swapping from a nominally performing subsystem
- Flight software change
- Hardware vulnerability
- Human safety
- Schedule/resource impact

The research described in this paper was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.
• First time in-flight event

It is important to characterize the risk items with respect to the approaching condition/event. For example, we can look at the second bullet above as it relates to concerns over an aging Inertial Measurement Unit (IMU) on the Odyssey spacecraft. In the near future, Odyssey will be supporting relay operations for the Mars Science Laboratory, which will require they have a functional IMU implying the need for a backup if the primary fails. Consequently one risk to the ability to support relay would need to be characterized in terms of how well each option supports maintaining a backup IMU. After identifying the risk drivers, the MA assessment proceeds to examine each of the options available to the project in terms of how robust each is in minimizing each risk.

Continuing with the Odyssey example, we would consider the options of waiting until the IMU starts to fail, waiting until it fails, or swapping while it is certain that some life remains on the IMU. If the project swaps IMUs once they get an indication of pending failure, there will still be a finite amount of life on the initial IMU to provide a backup capability. Waiting until an IMU fails and the spacecraft’s fault response swaps over, would leave no backup capability. Clearly a near term IMU swap would be most robust to this risk by leaving the greatest amount of life on the backup to respond to an unexpected problem with the new prime IMU. All the options are evaluated against each of the risk drivers. The MOAM then documents and compares the results of this evaluation using a suitable format. Often a matrix format is effective. Based on the results of this comparison, the MOAM provides the project with an assessment of the best option to select from the perspective of which is most robust to the identified risks. It is useful to identify both major and minor risk drivers.

A “major” risk driver is defined as having a significant impact on human safety or mission success. A “minor” risk driver is defined as not having a significant impact on human safety or mission success but improved the robustness of the operations. Now we can look at some complete examples starting with the Stardust case.

III. Under Cover of Darkness

The MOAM identified the risk drivers for the return options. These were gleaned from an examination of these daytime versus nighttime entry decision review areas.

• Earth Hazard Avoidance
• Ground Impact Hazard Assessment
• STRATCOM (The Air Force’s Strategic Command) Tracking
• Ground Station Coverage
• Downlink Data Rate
• Sample Return Capsule (SRC) Design Margin
• Ground Recovery Operations
• Backup Orbit Considerations

Taking these one at a time, we will discuss the relative risk of each option in terms of these areas.

Avoiding creating a hazard, particularly for the general population, upon the capsules return to Earth, is not surprisingly, a high priority. In an Earth hazard avoidance context, the proximity of targeting to Earth to the actual entry time is important. The closer to the entry date the spacecraft can be targeted, the smaller the error ellipse and thus the greater the probability of landing in the safe zone we are aiming for. In this regard, the nighttime entry has the spacecraft targeted to the Earth at E-13 days or 13 days prior to landing. For a daytime entry, it was necessary to target the spacecraft to Earth at E-30 days. From a human safety perspective, a nighttime entry is more robust in terms of minimizing risk to the population in the vicinity of the landing zone. The later targeting opportunity also reduces the window of vulnerability to uncontrolled Earth impact in the event of a catastrophic failure. Closely tied to the consideration of avoiding creating a hazard in the vicinity of the landing zone is the consideration of a hazard along the incoming ground track because of debris.

While no debris that would survive re-entry is anticipated with the SRC entry, it is prudent to consider the possibility in the event of an accident and assess the risks associated with each time of entry. Initial assessment shows a potential hazard track across two states, Utah and Colorado, for the nighttime entry. On the other hand, there is a longer potential hazard track across Canada and multiple states for the daytime entry. It is likely that this would have required some politically sensitive negotiations between the two State Departments necessitating additional effort by the Stardust team to provide further hazard risk information. Even though the track across western Canada was over sparsely populated areas, the total length of the potential hazard track and the complications of international negotiations do not add any positives to the risk adverse robustness of the daytime entry. Clearly, in terms of human safety during the entry overflight, the nighttime entry is more robust in terms of minimizing risk to human life as well as property. An available asset for determining how many objects (hopefully only one) are re-entering is STRATCOM’s space object tracking capability.
The STRATCOM Tracking resources for the nighttime entry include visual, infrared (IR) and radar skin tracking capability. For the daytime entry the only capability that can be used is the radar skin tracking capability. STRATCOM tracking is not required for determining the landing location of the SRC. Nevertheless, it does provide a valuable input in the event of some type of re-entry incident in providing information that can be responded to for dealing with potential hazards. STRATCOM’s tracking suite is clearly more robust to aid in mitigating risk from unexpected failure during a nighttime entry than during a daytime entry. Not only are we interested in an assessment of our ballistic performance, it is important to control and confirm events on the spacecraft, such as SRC release from the Stardust bus.

The team’s ability to control and confirm events for the SRC return is dependent upon reliable coverage by Deep Space Network (DSN) stations. In planning the communications approach for an event such as the SRC return, projects must consider the Jet Propulsion Laboratory’s (JPL) internal guiding design principles which state “the mission design shall ensure that redundant data paths not vulnerable to potential single failure(s) exist for real time return of flight data from post-launch mission critical events.” The principles go on to note that scheduling these events during periods of overlap between two DSN complexes is one means of satisfying this requirement. By planning critical events, such as SRC release from the Stardust mother-ship during a period when it is in view of two DSN complexes, we mitigate the risk of one station or complex being unavailable. While the likelihood of such unavailability is small, there have been instances of local equipment failure as well as complex wide issues with power or environmental forces, thus for a critical event, it is prudent to plan for redundant ground station coverage. Dual site coverage for SRC release activities for a nighttime entry is available from the Goldstone and Canberra DSN complexes from seven hours to two hours prior to entry of the SRC into the atmosphere. SRC release planned for four hours prior to atmospheric entry. For daylight entry there is a handover from the DSN’s Canberra complex to Madrid antennas at about 4 hours prior to entry. This means, not only can only one complex view the critical events, but they occur when one station is handing over tracking responsibility to another station, a far less ideal situation to maximize the likelihood of collecting the vital data we want. For the risk of not capturing the entry, descent, and landing (EDL) telemetry and of being able to command the spacecraft, clearly a nighttime entry is more robust. Closely associated with the coverage is the downlink data rate which determines how much data is available in real-time.

Two data rates were considered for the SRC return. Either one was adequate to downlink all the necessary data for the return and recovery. While it was possible to use the higher rate for the nighttime return but not for the daytime return, the fact that either would work made this a minor risk driver. It did of course contribute to the robustness of the nighttime entry contribution to mission success over that of the daytime entry. As a re-entry event, it also makes sense to consider how the SRC design margin can factor into the risk associated with each entry option. Entry velocity for a daytime entry is higher than the entry velocity for the nighttime entry option. This velocity difference translates directly into a delta in thermal loading between the daytime and nighttime entry options. The estimate for the impact of this is that about half of the SRC’s aerothermal margin would be used up by the increased entry velocity of a daytime entry. The established margin is maintained with the nighttime entry option. In terms of increased likelihood of re-entry survival and reduction of risk in this regime, the nighttime entry again provides the more robust option. Given the prior Genesis experience of a hard landing and capsule breach, the ground recovery operations encompass another major risk driver.

The concern with a compromised SRC is the time the samples from the comet Wild 2 would be exposed to moisture and possibly destroyed. If moisture were to contact the aerogel containing the sample material from the comet, these samples could be destroyed. In the event of a failure that resulted in capsule breach, time is clearly of the essence. It is certainly safer and quicker for crews to recover the capsule with the added visibility provided by daylight. Consequently we can conclude that the daytime entry provides the more robust response to the risks associated with a SRC breach and associated ground recovery efforts. The remaining area to examine deals with the potential that the decision is made not to release the SRC or there is a failure which precludes this happening and the entire spacecraft is placed in its backup orbit.

The backup orbit would return the SRC to earth for another re-entry try in a matter of years. From a Navigation and consumables viewpoint, either option enables a backup orbit with manageable Delta-V. However, a shorter backup orbit, by 2 years, is achievable with the nighttime entry over the daytime entry. The shorter timespan has the benefit of less exposure to the risk of spacecraft component failure over the longer orbit. While the fact that either approach provides a viable option for a backup orbit categorizes this consideration as a minor risk driver, we still conclude that the nighttime entry is more robust in terms of risk reduction.

We can examine a summary of all the considerations at once with the use of a simple and straightforward matrix below.

The research described in this paper was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.
The research described in this paper was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

### Risk Drivers and Rankings

<table>
<thead>
<tr>
<th>Risk Driver</th>
<th>Rank</th>
<th>Nighttime</th>
<th></th>
<th></th>
<th>Daytime</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Human Safety</td>
<td>Mission Success</td>
<td>Human Safety</td>
<td>Mission Success</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Earth Hazard Avoidance</td>
<td>Major</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ground Impact Hazard Assessment</td>
<td>Major</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRC Design Margin</td>
<td>Major</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ground Station Coverage</td>
<td>Major</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRC Processing Time - Anomalous</td>
<td>Major</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup Orbit Duration</td>
<td>Minor</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRC Release Downlink Data Rate</td>
<td>Minor</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>STRATCOM Tracking</td>
<td>Minor</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

✓: Lower Risk Option

Figure 1. Stardust Risk Trade Balance: Nighttime versus Daytime Entry

In examining Figure 1 above, we see that four of the five major risk drivers favor the Nighttime entry option as the lower risk option while one favors the Daytime entry option. To recap, the major risk drivers are:
- Earth avoidance strategy - favors a nighttime entry
- Ground impact hazard assessment - favors a nighttime entry
- Redundant ground station coverage - favors a nighttime entry
- The SRC design margin - favors a nighttime entry
- The recovery processing time for a breached SRC - favors a daytime entry

Further, the minor risk drivers add robustness with respect to risk mitigation for the Nighttime entry option. Not unexpectedly then that the Safety and Mission Assurance (SMA) recommendation stated that “On risk balance, preserving the SRC design margin by coming in at night and accepting a longer SRC processing time in the event of a breached SRC is recommended.” The project had initially planned for a Nighttime entry and concurred with the SMA recommendation proceeding with a Nighttime re-entry. We want to turn now from considerations of reducing risk for return of a capsule to Earth and consider the flyby of a comet by the recycled Deep Impact spacecraft for the EPOXI mission to Hartley 2.

### IV. Can You Hear Me Now

EPOXI is the extended mission for NASA’s Deep Impact spacecraft which uses the flyby part of Deep Impact. The impactor segment was released by the flyby spacecraft and collided with the nucleus of comet Tempel 1 on July 4, 2005. On July 3, 2007, NASA extended the Deep Impact mission, naming it EPOXI. The name EPOXI is a combination of the names for the two extended mission components: the extrasolar planet observations, called Extrasolar Planet Observations and Characterization (EPOCh), and the flyby of comet Hartley 2, called the Deep Impact Extended Investigation (DIXI). We will focus on aspects of the preparation for the Hartley 2 encounter.

The spacecraft attitude necessary to point the Deep Impact cameras at Hartley 2, necessitated use of the low gain antenna for the encounter with the comet. Following the encounter, it was important to switch to the high gain

The research described in this paper was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.
antenna and point it at the Earth to recover the encounter data as quickly and reliably as possible. The antenna switch could be accomplished in two ways. One option was to use the system as designed and select the antenna connected to the primary traveling wave tube amplifier (TWTA) using the waveguide transfer switch (WTS). The second option was to use one TWTA for one antenna and then swap to the other TWTA connected to the other antenna and thus not move the WTS. Since it was not the nominal approach consistent with the system design, why would we even consider the second option? As it turns out, earlier in the mission the downlink lost 8.5 dB of output power for a period of ~6weeks. The suspected cause was debris in the WTS, also referred to as foreign object debris (FOD). The threat to the spacecraft was that operating the switch could result in its getting stuck in a position that rendered the telecom system useless or degraded at best. The risk mitigation recommended was to stop using the WTS. To further complicate the situation, the helix current for TWTA-A began showing an increasing trend. The threat in this instance was that the TWTA-A would fail completely. Consequently, the risk mitigation was to select TWTA-B as the prime TWTA. As encounter drew closer, a third option emerged to have both TWTAAs powered on throughout the encounter period. These were the three options the MOAM had to include in their risk-balance study to develop a SMA recommendation for the project.

To begin the study, the MOAM identified the risk drivers for the return options. These were gleaned from an examination of these telecom configuration decision review areas.

- Telemetry visibility during Closest Approach
- Hardware vulnerability
- Schedule/resource impacts
- Executing a first time in-flight event

Examining these individually, we will discuss the relative risk for each of the three options in terms of these areas.

JPL’s internal Design Principles requirements document for flight projects states that “The mission design shall provide for a real time downlink capability during mission critical events.” This applies for extended missions as well thus it is an important area for the MOAM to examine. Two of the options can provide full visibility throughout the closest approach time frame. By exercising the WTS, the time to switch between antennas is very nearly zero, so there would be no real loss of visibility of activities. Similarly, having both TWTAAs powered means simultaneous transmission through both antennas and consequently no loss of visibility during this time period. The least robust option is the TWTA swap. When you actually command a swap, because of warm up time and command restrictions, there is a five minute period when neither TWTA is operating. Since this would occur two minutes after closest approach, the visibility for closest approach is maintained, but there is a gap in visibility shortly after the event. In considering the three options, we see that the TWTA swap is the least robust for the risk of visibility loss while the other two options are equally robust in terms of risk mitigation. Of course there are additional considerations such as the risk to hardware of the options that we must look at.

As previously discussed, there are concerns about the telecom system which is vital for the success of the EPOXI encounter. The two areas are the potential for TWTA-A failure and the malfunction or non-function of the WTS. The concern for TWTA-A is based on the increasing trend of the TWTA-A helix current which could indicate an impending failure. Also as discussed, the concern for the WTS stems from the investigation of a loss of output power by 8.5 dB over about a six week period. The investigation concluded that the likely cause was FOD in the WTS. Both of these do play together in considering the risk driver relating to hardware vulnerability. If TWTA-A were to fail, the spacecraft fault protection would swap TWTAAs to TWTA-B. We would experience the 5 minute warm-up outage at the point of failure that was discussed earlier for the option of swapping TWTAAs after closest approach. However, the control of which antenna TWTA-B connects to would be through the WTS which is a concern of its own. So if TWTA-A failed prior to closest approach, the low gain antenna would be switched to TWTA-B using the WTS and TWTA-B powered on, then after closest approach the WTS would be exercised again to connect TWTA-B to the high gain antenna. During the extended mission, the TWTAAs were swapped between A and B a total of nine times. For the swapping TWTAAs option, unless there is a TWTA-A failure, there is no exposure to the WTS anomaly risk. Further, TWTA-A has not exhibited any actual failure symptoms and the swap between TWTAAs has been exercised during the extended mission. The option of using only one TWTA and using the WTS to reconfigure the telecom system between the low gain and high gain antennas is not recommended by the Telecom Anomaly Review Team due to risk of FOD jamming the WTS resulting in potential loss of mission. The WTS was operated after anomalous 8 dB power drop on TWTA-B but that was prior to determination of FOD as most probable cause for the power loss. This option is robust to the TWTA-A failure risk, but remains vulnerable to the risk of a jammed WTS which could result in mission loss. The third option of operating both TWTAAs simultaneously appears feasible. It was not thoroughly studied, but initial assessments indicated that it could be supported from a power perspective. Questions about thermal impacts remained to be answered as well as any possible interference between the antenna patterns. Without some modification of on-board fault protection

The research described in this paper was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.
responses, it is not clear that a failure of TWTA-A might result in exercising the WTS to put the low gain on TWTA-B, at least until after closest approach and then taking the risk of exercising the WTS again to reselect the high gain antenna for recovery of the encounter data. This option seems somewhat neutral with respect to hardware vulnerabilities, but the unknowns on thermal and fault protection changes do not help it stand out as really robust with regards to this risk. Another area for consideration is schedule and resource impacts which become a concern with the option of having both TWTAs on throughout the encounter.

As an extended and discovery class mission, EPOXI is resource limited and at the time of this decision, there is little time left in the schedule to develop new techniques, processes, or sequences. The encounter sequences to control the spacecraft activities must be developed and thoroughly tested to ensure that they will execute as planned and perform the functions intended. Further, staffing is limited given that the flight team is not the team originally developing flying Deep Impact, especially in the sequencing area. To minimize the risk of an error in a sequence, it is important not to perturb the development schedule or add too much to it. The option to swap TWTAs at encounter plus two minutes is the baseline plan. Choosing this option would not perturb the current schedule or add to the workload of the sequence development and testing team. The option to switch antennas using the WTS is not a new approach. It has been done in flight and sequences have been built to perform this function in the past. Consequently, if the decision is made in the near term to take this approach, the impact on schedule and resources would be quite small. The newest option, performing the encounter with both TWTAs powered hasn’t been sequenced in the past. From a command perspective, this would require the development and testing of new sequences to perform an activity that has not been performed in the past. Development of new sequences would be a significant increase in resource usage and schedule consumption. If unanticipated problems are encountered or if the approach proves impractical, the team would have to abandon this approach and revert to one of the other options. Such a situation would result in a considerable waste of schedule time and personnel resources. Given that the baseline plan was to swap TWTAs, that option is the most robust in terms of minimizing risk to resources and schedule, followed closely by the WTS usage to reconfigure the telecom system. Above we alluded to the final area to examine when we alluded to the fact that keeping both TWTAs powered on had not been performed in the past. It would be a first time in-flight event.

While it is necessary shortly after launch to perform events, such as deployments, valve firings, and check outs, for the first time in-flight, it is not something to be taken lightly. Indeed the initial post launch first time events were thoroughly reviewed and tested prior to launch. As the mission progresses, the attractiveness of performing an activity for the first time becomes less and less appealing. There is, of course, the inherent risk of an error in a sequence that could not be found by ground testing on a simulator that just cannot duplicate the spacecraft performance with absolutely 100% accurate fidelity. There is also additional overhead of extra reviews and testing, the results of which must be carefully reviewed followed by more testing and reviews. The preference is to avoid the risk of doing something for the first time whenever possible and the swapping TWTAs and using the WTS options are both robust in this regard, while having both TWTAs on is not. We can examine the options side by side with respect to their risk to mission success (++ indicates robustness to risk) in the matrix of Figure 2 below.
The research described in this paper was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

<table>
<thead>
<tr>
<th>Risk Drivers and Ranking</th>
<th>Risk Trade Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Drivers</strong></td>
<td>Rank</td>
</tr>
<tr>
<td>Telemetry Visibility during closest Approach</td>
<td>Minor</td>
</tr>
<tr>
<td>Hardware vulnerability</td>
<td>Major</td>
</tr>
<tr>
<td>Schedule/Resource Impacts</td>
<td>Major</td>
</tr>
<tr>
<td>In-flight First Time Event</td>
<td>Minor</td>
</tr>
</tbody>
</table>

✓: Lower Risk Option

**Figure 2. EPOXI Risk Drivers: Encounter Telecom Configuration**

This is certainly a close call with the switching of TWTAs having a slight advantage from a risk perspective. We should note that from a risk perspective, the telemetry visibility issue comes into play more for the reconstruction of events in the case of an incident during the encounter. For that reason it is included as a Minor Risk Driver. In-flight First Time Event is also considered a minor driver because there is a well-defined and thoroughly vetted process at JPL to minimize risk for first time events, but, of course, no process is absolutely guaranteed to work perfectly. The SMA recommendation was based on overall risk balance and was to switch the TWTAs which maximizes the likelihood of mission success while accepting a 5 minute telemetry gap starting at closest approach plus 2 minutes. This is the option that was successfully utilized for the EPOXI encounter with comet Hartley 2. In both the Stardust and EPOXI cases, the risk balance study supported the original plan that the project had in place, but that is not guaranteed.

**V. Conclusion**

To maximize the likelihood of mission success, we must drive risk to as low a level as feasible. While we make every effort pre-launch to mitigate risk, there will always be some residual risk throughout the mission. There can also be new risk as the result of hardware failures or changes in the environment as the result of an extended mission that differs from the original mission. Changes in the mission’s risk posture or even a change in the review authority for mission activities can prompt a reassessment of plans for key mission events. The two cases we considered above demonstrate this clearly.

The Stardust plan for a nighttime reentry was reexamined after a concern was raised about human safety. This had been addressed initially, but the perception of daytime versus nighttime safety prompted the project to reconsider their approach. EPOXI was in a different environment for its extended mission and had experienced a number of hardware concerns since the conclusion of their primary Deep Impact mission. The attitudes prompting

The research described in this paper was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.
antenna switching and the concerns about TWTA and WTS performance prompted the project to reconsider their initial plan for telecom configuration. In both these instances, the SMA recommendation mirrored the original project plan. That is not always the case as in the Odyssey case that was mentioned in the background section.

In the Odyssey case, the project initially recommended an immediate swap of UHF radios and IMUs. The SMA recommendation was to wait until some indication of IMU degradation was observed. Based on programmatic considerations, the project was directed to not do an immediate swap. This decision was later reinforced by additional information on IMU lifetime and failure mode which effectively gave the project more time to plan a transition from one side to the other once they saw the signature of impending IMU failure. Whether or not the recommendation of SMA matches the original project plan or not, the importance of doing the risk balance study is to make sure the risks are properly considered and evaluated.

We have found that the conduct of these studies helps to ensure that the event is carefully considered in terms of what risks are posed by each option and assists the project in maintaining focus on mission success. Recall from the definition of mission success that it includes recognition that there will be risk, and also the caveat that the risk which is accepted shall be reasonable. The purpose of the risk balance is to ensure that the residual risk for an event is reasonable and we have been successful to date. The risk balance study is being incorporated as a tool at JPL for MOAMs to use with their flight projects to aid them in promoting risk awareness and appropriate risk management for flight projects throughout both primary and extended missions.

References