5. RISK MITIGATION

The following discussion gives an account of how changes in Operations early in the mission planning stage resulted in a cost-effective mitigation of risk.

5.1 Introduction

In the EO-1 mission, there were five instrument and seven spacecraft technologies to flight-validate during one year of baseline operations. EO-1 operations and the accompanying ground system were intended to be simple in order to maintain low operational costs. For purposes of formulating operations, it was initially modeled as a small science mission. However, it quickly evolved into a more complex mission due to the difficulties in effectively integrating all of the validation plans of the individual technologies. As a consequence, more operational support was required to confidently complete the on-orbit validation of these new technologies.

It is interesting to note that the realization was made late in the mission planning, at a point in time, whereby changes on the spacecraft and instruments were constrained and that the only viable area to retain a margin of flexibility was in the area of operations. Therefore, since it is much easier to de-staff than to find and train knowledgeable personnel, it made sense to overstaff operations from the beginning of the mission with the idea that any extra cost accrued by operational personnel pales in comparison to changes required on the spacecraft and the instruments. This in effect became the cost-effective risk management approach.

5.2 Scope

There were three instrument groups who needed to validate their instruments individually and there were over 80 validation scientists working with the Science Validation Facility (SVF)/Mission Science Office(MSO) to get images to validate their respective science. To minimize the work done by operations, it was decided that for the majority of the time, all three instruments would image simultaneously and all the data which included meta-data (engineering data about science data), would be included on one Digital Linear Tape (DLT) tape which would be duplicated and distributed to everyone. This approach required that there be tight coordination between all of the scientists and instrumenters to work a master scene list which prioritized the scenes. The planning process then placed the scenes that the most scientists would benefit from early in the mission. This meant that in general, if there was a scene that two or more scientists need, it would be taken before one that only served one scientist.

5.3 Operations Selected as Buffer to Risk

As risk aversion rose in the Agency, it was clear that assurances were sought that the mission's chances for success were being maximized. But in order to do that, mission success had to be defined. A model was created that defined success in a stepwise manner. Figure 6 shows the success criteria for the EO-1 mission. It is depicted as a bar graph with success ranging from minimal success, defined as the completion of certain validations, to complete success, which consists of completing all of the validations. For example, in order for the EO-1 mission to be minimally successful, the Advanced Land Imager had to be successfully validated. In order for that to happen, the Wideband Advanced Recorder Processor (WARP), the science data recorder, had to function reliably. The WARP, although not a Category I technology was classified as Category II without which the Category I technologies could not be validated.

Once the success model was created, the next step was to assign probabilities of success. This was achieved by creating a spacecraft reliability curve as depicted on Figure 7. The curve in Figure 7 was created from underlying reliability for each of the spacecraft subsystems. Figure 8 shows the calculation for reliability for each subsystem based on a Failure Mode and Effects Analysis (FMEA) that was conducted late in the mission development lifecycle. Each block in Figure 8 has an underlying analysis, which is comprised of historical parts failures which were then tallied to get the aggregate reliability for each box.

Once the success model was created, along with some probabilities of success, decisions were made as to how to maximize success based on this model. For example, in Figure 9, by moving some of the validation work into the

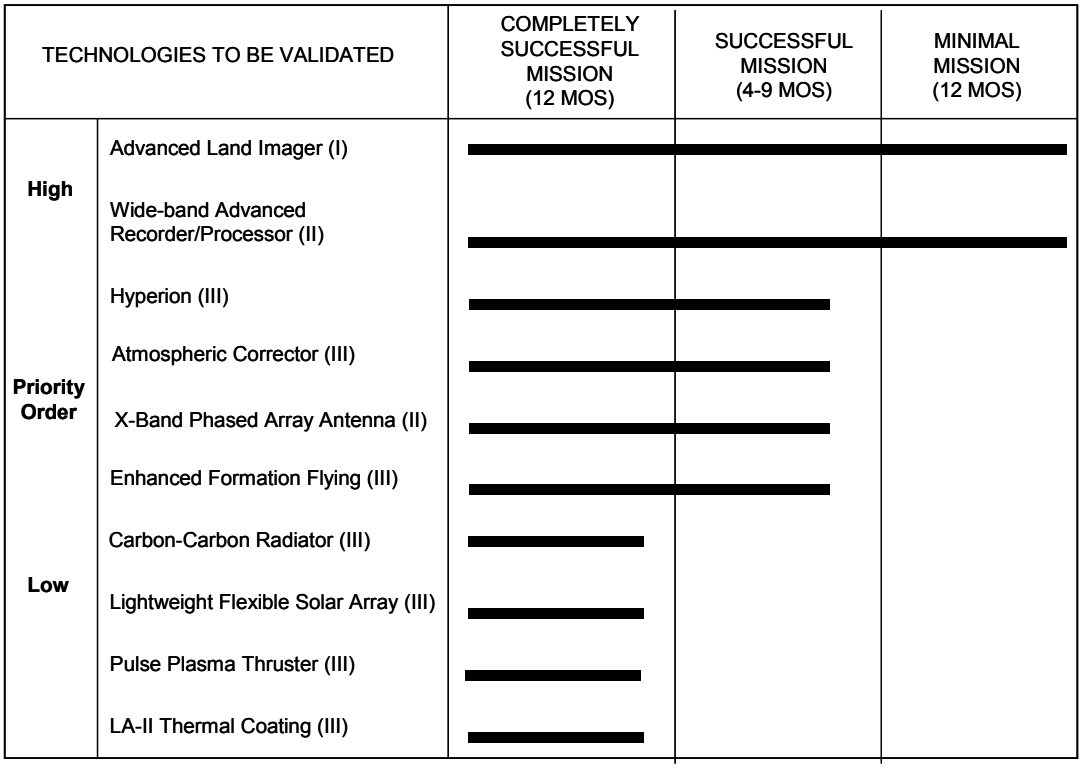

Figure 7 – EO-1 Mission Success Criteria

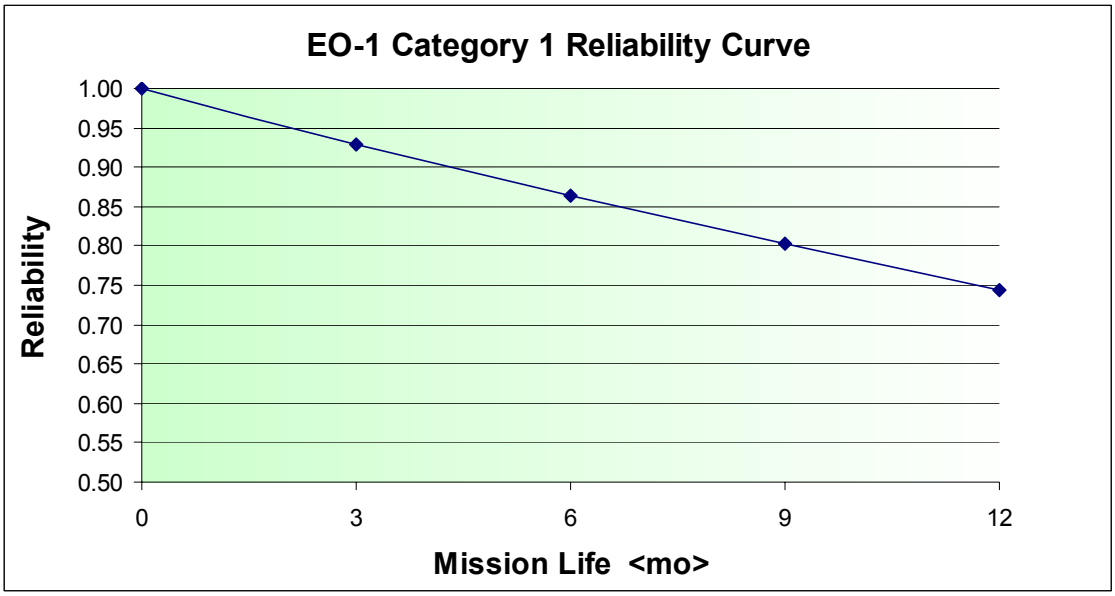

Figure 8 - EO-1 Mission Reliability

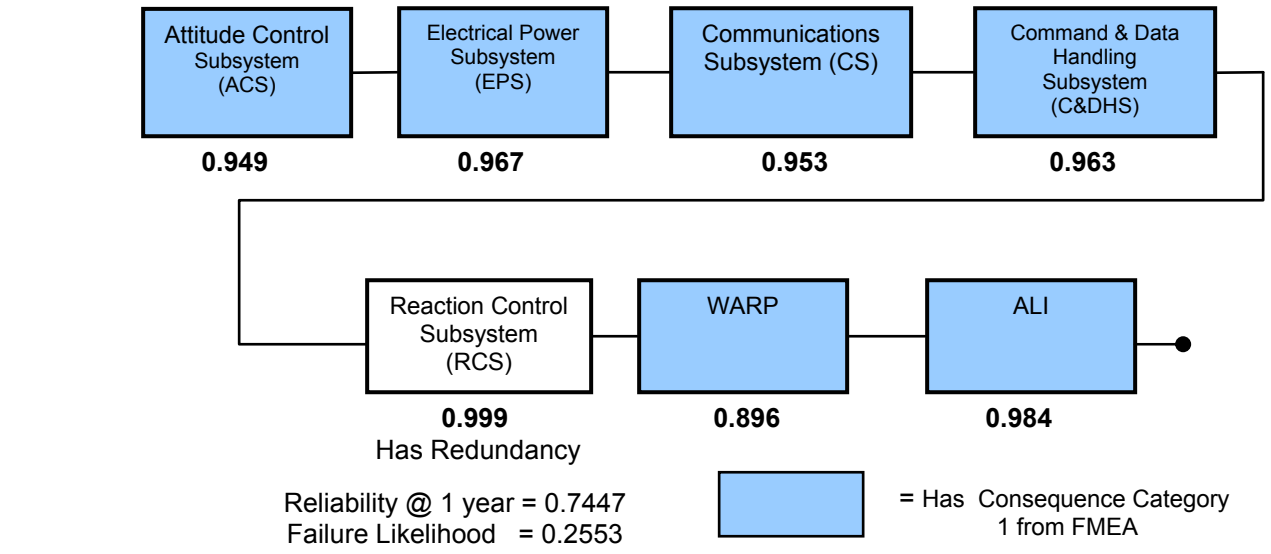

Figure 9 - Calculated Reliability for Each Subsystem

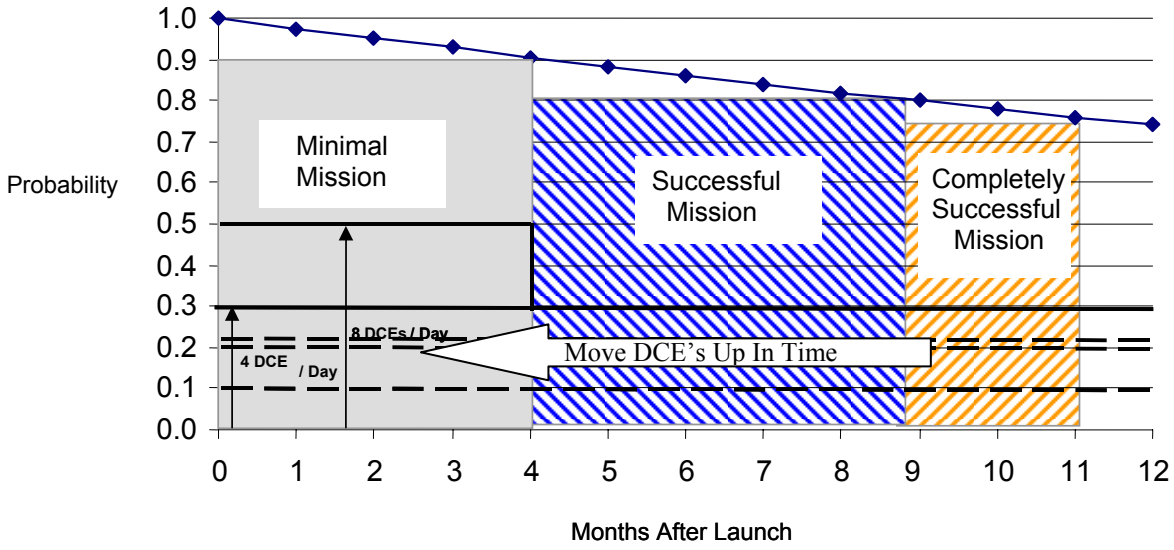

Figure 10 - EO-1 Mission Reliability and Mission Success Criteria

earlier part of the mission, the probability of getting at least minimal success was increased. Figure 9 shows a graphic of

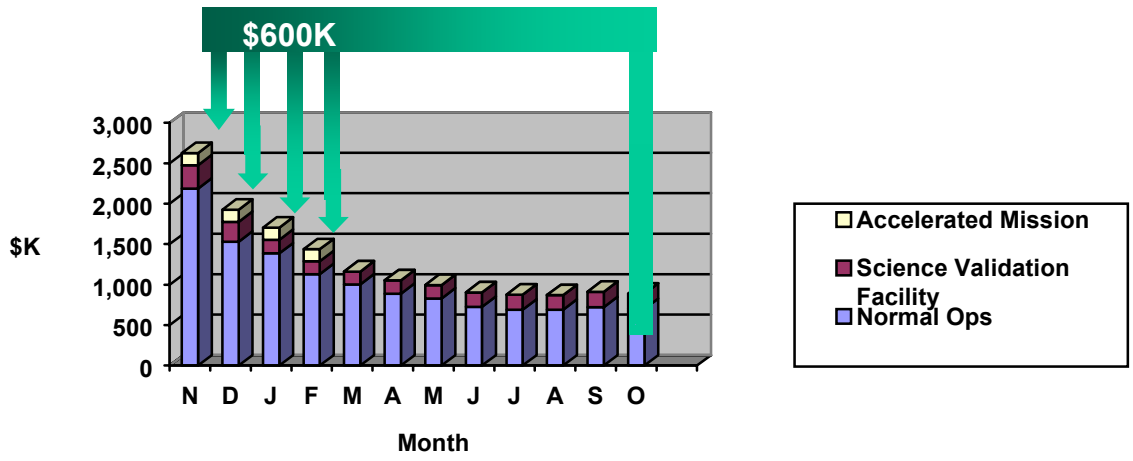

Figure 11 - EO-1 Accelerated Mission Approach Using Operations Augmentation

mission success versus mission reliability. The arrows depict work moved up in time so that the work lies under the more reliable part of the curve. In this case, the work moved up in time is that of taking Data Collection Events (DCEs) that were scheduled for later in the mission, into the first 120 days. By doing this, operations was required to take 8 DCE's per day versus 4 DCE's per day thus doubling the work and at least doubling the complexity of operations. The DCE's that were moved up were those that represented the ones needed to minimally complete the validation of the ALI. Thus, the probability of completing all of the DCE's to complete the mission in a minimally successful way was increased from a probability of approximately 75% up to 90%. Of course, the question was what would be the cost to implement this change in operations. Figure 10 shows the added cost of shifting to this 8 DCE per day mode. It turned out that for $600K extra, the task could be accomplished and thus place the minimal validation portion of the operations under the higher probability values. Furthermore, by using the money in month 12 to fund the difference, management had the option of either completing the mission within the specified budget or providing more money to extend the mission.

This approach was weighed against other approaches to provide increased reliability for the mission. It turned out that this approach was far and away the most cost-effective approach. For example, at the Red Team Review late in the development cycle, the question was asked if there was a way to reduce the risk of failure of the WARP, the science data recorder. An effort was initiated to see what it would take to create a partial backup second string for the WARP. Without the WARP, it was almost impossible to achieve minimal success despite the WARP not being a Category I technology. At the time of the analysis, this course of action would have introduced a launch delay. At $1.5 million per month, the mission cost would quickly increase. In addition, there was the added risk that the necessary testing of the WARP backup could not be accomplished successfully.

Of course, had this proposal been made near the beginning of the mission, then the choice that would have been made would probably have been to build this backup to the WARP. Given the cost and risk to achieve added reliability late in the mission, the operational approach depicted here was selected instead.

By launch, EO-1 had been though approximately 40 reviews Many decisions like the one above were made late in the mission as a result of questions asked in reviews and resultant actions. By having the success model, the mission office was easily able to select changes in the operational approach by being able to weigh the risks and costs of alternate approaches.

5.4 Changes to Operations

The initial operational concept called for 3-5 people on the Flight Operations Team (FOT) pre-launch and 2-3 people post-launch during nominal operations. Over the next couple of years, risk tolerance changed and there was increased interest in mission results. This caused a change from doing an 8 hr by 5 day operations approach for normal operations to 24 hour operations, 7 days a week. But these changes had to be evaluated in light of achieving mission success. Whereas the original operational concept called for a very low cost, single string mission with lights-out operations, the evolution to the operations concept eventually used included adding the following elements each of which added cost to the development of operations:

a. More stringent security
b. ISO 9000
c. Change of operations contract to CSOC
d. Development of a S/C User's Guide
e. Development of well documented contingency procedures
f. Increased hours of S/C experience by MOC
g. Increased simulations
h. Increased training on S/C, instruments and ground, especially in the area of contingency and constraints
i. Hired higher level, more knowledgeable FOT personnel
j. Hired console operators instead of allowing the Operations Engineer to man the consoles. This allows for Operations Engineers to be freed up to focus on the anticipating problems versus worrying about day to day operations

Previous small missions at Goddard did not do evaluations on probability of success. But as the various reviews in the approximately 40 independent reviews proceeded, it was clear that the reviewers appreciated the ability to measure decisions with these metrics and furthermore, knowing this information tended to cause them to swing towards a more conservative approach, demonstrated in part by the changes mentioned above. Also, the independent reviewers enthusiastically endorsed the accelerated mission (moving DCE's up in time) as the most cost-effective way to manage risk.

A significant driver for the quicker turn-around of the mission was the necessity of timely validation due to the desire to maximize technology infusion opportunities. To operations, this originally translated into "quickness is more important than risk". With this in mind, and trying to keep costs very low, other technology activities were tightly folded in between imaging activities. Further complexity was added by adopting a plan to compress the "minimal" mission into 120 days instead of one year to take advantage of the increased reliability of the spacecraft early in the mission.

In sum total, the required changes can be categorized into the following few categories of change drivers.

1. Change of risk tolerance

In an early review, the Mission Manager stated, "Risk is what the EO-1 mission is about". The original concept for EO-1 was that by taking high risk, cost could be kept low. For example, the original operational concept called for running EO-1 with only two FOT members. But events conspired to change that approach. In particular, after the NASA Research Announcement, there was more interest in the science community than initially anticipated. As customer interest increased, risk tolerance decreased. Furthermore, this was further amplified by near time frame NASA mission failures.

This decrease in risk tolerance translated into a number of new activities that were not originally planned for as follows:

a. Generation of a Spacecraft User's Guide (over 2000 pages) by the FOT with the support of the subsystem engineers
b. Training of the FOT on all of the subsystems by subsystem engineers
c. Implementation of ISO 9000 documentation standards including generation of a product plan
d. More formalized documentation was placed on a website and then required a significant web effort to maintain
e. Implementation of network security. Originally, the Mission Operations Center (MOC) was on open IOnet, however, we have now developed a plan whereby remote access to the MOC is achieved by having a firewall which

checks a password that changes every minute in addition to validating that the IP address from which the user is logging in is a valid one.

f. Implementation of dedicated 256 kbps lines to TRW and Lincoln Lab so that they could monitor instrument activities remotely with an ASIST workstation (same as in the MOC)
g. Increased trending requirements
h. Leaning away from use of automation as originally planned to allow for 5 day x 8 hour operations. This mode of operations was evaluated post-launch + 30 days to examine its viability
i. Going from what originally was two seats with two workstations and one front-end in a portion of the MOC for Earth Science Data and Information System (ESDIS) project to a facility which has 10 workstations, 8 or so X-Terminals, and a separate data processing room. FOT staffing increased from the original proposal of 2-3 to 16 for normal operations (accelerated mission).

There was also the traditional discussion as to whether to test safehold on orbit with the fear that once in safehold, we might not be able to get out. But due to the fact that EO-1 is single string, it was decided that safehold would be tested early while all of the subsystem engineers were still available and easily accessible.

2. Single string spacecraft design approach

EO-1 was originally conceived as a single string mission and was modeled for purposes of budgeting and sizing, as a small science mission. It was designed as a single string mission with the idea that less complexity would mean shorter schedules and lower cost. But despite the fact that time was saved in Integration and Test of the spacecraft, almost no time was saved for operational testing because the major part of operational testing occurred with the first box while the second backup box was quickly tested.

But where the single string approach impacted operations the most was in the development of contingency procedures. Because there were fewer safeguards built in, more knowledgeable and more experienced operational personnel had to be hired. This allowed for contingency procedures to be more stringently designed and better tested. Also, this drove the need for more training and simulations than would otherwise not be deemed to be necessary. In fact, by launch, EO-1 had operated the spacecraft from the MOC for over 1300 hours and had over 800 hours of simulation rehearsals. Compare this to the original plan of 180 hours of operating the spacecraft from the MOC and maybe 200 hours of simulation rehearsals. Much of this was driven by the fact that we did not have a high fidelity simulator. For the EO-1, the "simulator" was flown. But this was deemed to be more cost effective since high fidelity simulators can cost millions of dollars.

3. Compression of mission timeline

As mentioned earlier, the revised approach was to complete the "minimal" mission in 120 days. This translated into taking more scenes per day. Originally, when the number of scenes to be taken and processed was to occur in one year, it was felt that there was enough flexibility that automation could allow an 8 hour by 5 day operation. This included a portion of a person to do planning. However, with this revised plan of taking up to 8 scenes a day, the scientists were busy prioritizing the targets from the available ground track of the spacecraft. They requested that we take a look at taking multiple scenes on an orbit whereas before we would only take one scene per orbit. The complexity in trying to achieve this is that momentum management to control jitter takes up to 40 minutes per scene, downlink opportunities are limited, and EO-1 only passes over the U.S. on 3 of its 14 orbits per day. As a result, it takes 3 people to do the planning versus the original single planner.

4. Increased controls needed on team

EO-1 originally was designed as a small tightly knit team with a high level of communication between the various elements such as operations, subsystem engineers, technologists and scientists. For a small group this allows for great cost savings and avoidance of some documentation and management controls such as large, formal Change Control Boards. But as the team grew and risk tolerance diminished, there came a threshold whereby the need arose for more formalized mechanisms of control. This resulted in the creation of four Configuration Control Boards (CCB); a Mission Level CCB, a Flight Software CCB, an Operations CCB and Integration and Test CCB. Needless to say, many team members were required to attend multiple board meetings. Furthermore, contractor personnel were added to help process the paperwork.

The team still retained a high level of informal communications between I&T, Operations, and the technologists due to the

fact that the same people worked side by side in both I&T and the ongoing simulations. This was necessitated by the fact that, whereas for most missions the spacecraft manufacturer runs the launch, for EO-1 the Mission Systems Engineer and Mission Technologist led the launch effort. This added an overhead burden on EO-1 personnel but added a higher degree of confidence that some small change would not impact the mission.

5.5 Lessons Learned Applications

After reviewing some of the lessons learned on EO-1, it was agreed that the first thing to do on this type of mission is to do a reliability assessment using such tools as FMEA, Fault Trees and Probability Risk Assessment. Then based on the analysis, design the spacecraft with selective redundancy to minimize risk where it is cost-effective. Once this is done, then do the following:

a. Estimate the operations staffing needs and then overstaff to provide a risk management buffer to be able to handle unexpected requirements and changes in risk tolerance.
b. Estimate range of operational activities depending on risk events and provide adequate flexibility through contract mechanisms such that, as the need arises, FOT members can easily be obtained.
c. Another problem encountered was the need to expand facilities as more personnel became required. Therefore, set up facilities so that they can easily be expanded.
d. Finally, gain early access to web-based management tools to allow for flexibility to transition to a more rigorous team control mechanism as needed.

5.6 Conclusion

By viewing the mission using risk as a metric and with various levels of success criteria, the mission team was able to better perform tasks on the priority of importance. That is, DCE's and technology validation deemed more important were done earlier than those of lower priority.