Expected Productivity-Based Risk Analysis in Conceptual Design: With Application to the Terrestrial Planet Finder Interferometer Mission

by

Julie A. Wertz

S.B. Aeronautics & Astronautics
Massachusetts Institute of Technology, 2000

S.M. Aeronautics & Astronautics
Massachusetts Institute of Technology, 2002

SUBMITTED TO THE DEPARTMENT OF AERONAUTICS & ASTRONAUTICS IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTORATE OF PHILOSOPHY IN AERONAUTICS & ASTRONAUTICS
at the
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

FEBRUARY 2006

Signature of the Author: _____
Department of Aeronautics and Astronautics
December 30, 2005

Certified by: _____
Professor David W. Miller
Department of Aeronautics and Astronautics
Thesis Supervisor

Certified by: _____
Professor John J. Deyst
Department of Aeronautics and Astronautics

Certified by: _____
Dr. Raymond J. Sedwick
Department of Aeronautics and Astronautics

Certified by: _____
Dr. Hamid Habib-Agahi
Jet Propulsion Laboratory

Accepted by: _____
Jaime Peraire
Professor of Aeronautics and Astronautics
Chair, Committee on Graduate Students

Expected Productivity-Based Risk Analysis in Conceptual Design: With Application to the Terrestrial Planet Finder Interferometer Mission

by

Julie A Wertz

Submitted to the Department of Aeronautics and Astronautics
on November 1st 2005, in Partial Fulfillment of the
Requirements for the Degree of
Doctorate of Philosophy

Abstract

During the design process, risk is mentioned often, but, due to the lack of a quantitative parameter that engineers can understand and trade, infrequently impacts major design decisions. The definition of risk includes two elements – probability and impact. As a result of heritage techniques used in the nuclear industry, risk assessment in the aerospace industry is usually purely reliability based, and is calculated as the probability of a failure occurring before the end of the design lifetime. While this definition of risk makes sense if all failures result in the same impact, for many non safety-critical systems, the impact of failures may vary, including variance by when a failure occurs. While current risk assessment techniques answer the question "What is the probability of failure?", the true question that needs to be answered for many missions is "How much return can be expected?" Depending on the question answered, the relative ranking of risk items may be different – leading to different risk mitigation investment decisions. Consequently, to complete an accurate risk assessment, it is important to combine system performance and reliability, and model the probabilistic nature of the expected value of the total system productivity. This expected value is defined as the expected productivity.

While the expected productivity is easy to calculate for simple systems, it is more complex if a system has a path-dependant productivity function, as is the case with many aerospace systems. In these systems, the productivity in each state depends on the previous states of the system. An approach, called Expected Productivity Risk Analysis (EPRA), has been developed to model the systems described above in an efficient manner by finding the expected path, and then find the expected productivity given that path. EPRA has been tested against conventional Monte Carlo simulations with excellent results that consistently fall within the 95% confidence interval of the Monte Carlo results, while completing the simulation up to 275 times faster. The EPRA approach has been applied to two case-studies, to demonstrate the importance of using expected productivity in a trade study for a real mission, the Terrestrial Planet Finder Interferometer.

Thesis Committee Chair: David W. Miller, Sc.D.
Title: Associate Professor of Aeronautics and Astronautics
Director Space Systems Laboratory

Thesis Committee Member: John J. Deyst, Ph.D.
Title: Professor of Aeronautics and Astronautics
Department of Aeronautics and Astronautics

Thesis Committee Member: Raymond J. Sedwick, Ph.D.
Title: Principal Research Scientist
Department of Aeronautics and Astronautics

Thesis Committee Member: Hamid Habib-Agahi, Ph.D.
Title: Principal Engineer
Jet Propulsion Laboratory

Thesis Reader: Cyrus D. Jilla, Ph.D.
Title: Space Systems Engineer
SRA International

Thesis Reader: Col. John E. Keesee
Title: Senior Lecturer
Department of Aeronautics and Astronautics

Acknowledgements

This research was supported by the Michelson Fellowship program through the Michelson Science Center operated by the Jet Propulsion Laboratory. The support of this sponsor is gratefully acknowledged.

There are several additional people and organizations that I need to thank for their support and help throughout the research process. All of their contributions made this work not only possible, but also fun – and I am deeply grateful to all of them.

First of all, I must thank my committee. Dave Miller has been my research advisor throughout my entire graduate school experience. He has a talent for allowing students to have independence and discover both problems and solutions on their own, while all the time knowing that if they ever can't figure something out, Dave will be there to step in. My JPL supervisor, Hamid Habib-Agahi, has been exceptionally supportive. Without his support, doing this research while at JPL would not have been possible. I truly appreciate his willingness to let me work on my research without applying pressure to do additional projects. My minor advisor, John Deyst, was also very supportive of the research and encouraged me to be creative and to find new ways to grow and solve problems. Finally, Ray Sedwick, provided both general support and a keen critical eye to ensure that the problem and the solution that I was working on were both practical and technically correct.

This research was conducted for the Massachusetts Institute of Technology, while sitting in residence at the Jet Propulsion Laboratory. This situation was both very unique and very beneficial – in terms of both the final research product and my personal situation. Without the support of members of both institutions, working on my research while 3000 miles away from my school would not have been possible. I truly believe that the models that were produced, the motivation behind using expected productivity, and even the case-studies presented in this research would not have been nearly as well developed without the ability to sit down regularly with the TPF-I team, as well as with engineers doing work on other JPL missions. I am truly grateful for being given this unique opportunity, and hope that the experience can be repeated for other students in the future. Specifically I would like to thank Dave Miller, Hamid Habib-Agahi, John Deyst, Ray Sedwick, Tony Freeman, Erik Nielson, John Crawford, Curt Henry, Chuck Weisbin, Marie Stuppard, and Marilyn Good for making this situation possible.

The TPF-I team provided invaluable information and support throughout this research process. They took me in as an unconditional member of the team, for which I am extremely grateful. I only hope that the products of my research provide them with some new and useful information in return for the support they provided to me. Specifically, I would like to thank Curt Henry, Louise Hamlin, Oliver Lay, Serge Dubovitsky, Doug Adams, Asif Ahmed, Dave Fisher, Steve Gunter, Stefan Martin, Dan Miller, George Purcell, Zahid Rahman, and Jeff Tien.

I received technical advice and support from many people throughout this process. Cyrus Jilla has been a mentor throughout my entire graduate school career. His wealth of technical, professional, and personal advice has been invaluable to me throughout the past 5 years. In addition, Cyrus was a great help as both an outside examiner on my general exams and an outside reader for my thesis defense. I truly appreciate his taking the time and making the trip to Boston to be there for both events. The other outside reader for my thesis was Col. John Kessee. Col. Kessee has provided both technical advice and a warm smile to students all across MIT, including myself, and I greatly appreciate his help and support. Oliver Lay has been unbelievably kind and patient with me throughout the years. Oliver has taken time out of his schedule to sit down and explain the concepts of interferometry numerous times over the past several years. He has done an amazing job of explaining a very complicated subject and I truly appreciate his time, effort, and support. Leila Meshkat has been a wonderful mentor and guide into the risk world at JPL. She has taken the time to meet with me on a regular basis and discuss all aspects of what is occurring throughout the "risk world" – and I appreciate the time and interest she has taken in my work. Alberto Elfes provided a large amount of knowledge and guidance in terms of mathematical approaches and new methods of quantitatively completing a risk analysis. His support of my work by finding me a task at JPL that was complimentary to my research was both very kind and extremely helpful. Chuck Weisbin also provided incredible support for my work by allowing me to work part-time on tasks while I worked on my research. His support made it possible for me to not only work part-time at JPL, but also work on truly interesting assignments. Jeff Smith also contributed greatly to me being able to work on very interesting part-time tasks while working on my research. In addition, Jeff provided a large amount of advice about getting through a Ph.D. program, how to deal with complex and somewhat "fuzzy" problems in a quantitative way, and interview techniques and methods for extracting information from expert sources. Finally, Al Chen has provided immeasurable advice and support throughout this process. He has become a risk expert in his own right, and has provided me with technical support ranging from editing my thesis to giving advice on how to keep any solution I developed practical and useful on real flight missions.

As I mentioned above, I have had fun throughout this process. This is due entirely to the wonderful people I work with and my incredible friends – on both sides of the country. All of the people at JPL have been a blast to work with and have put smiles on my face day in and day out. While everyone has been amazingly fun to work with, there are a few people in particular that I would like to thank. Milana Kozulina has been the best office mate I could have asked for. She has kept me not only sane, but also entertained for the past three years – and become one of my closest friends in the process. Two of our "unofficial office mates", Theresa Kowalkowski and Leila Meshkat, have also helped keep me sane throughout this process. Our morning and lunch time chats have gotten me through more than one tough day when the research just wasn't going well, and our girls' nights out/in have been, and hopefully will continue to be, extremely fun. Thanks so much to all three of you for all the talks, the laughs, the advice, and the support. Tibor Balint has also provided constant entertainment and a new and interesting

perspective on many issues. His random jokes and gifts from exotic places, like Albuquerque, always provide a laugh.

While many people left the SSL since I started the Ph.D. program, I still have many good friends that provided a huge amount of support back in Cambridge. Steve Sell has let me crash on his couch every single time I went back to MIT. He's listened to me complain and stress about research every trip, and still invited me back the next time – and I truly appreciate both the bed to sleep on and the friend to listen. Becky Masterson has also been a great friend and a great support to lean on. She has provided huge amounts of invaluable advice on the Ph.D. process each step of the way. Shannon Cheng, Shonna Coffey, Joe Pacheco, Chris Salthouse, and Lucy Fang have been some of my closest friends throughout my entire MIT experience – from freshman year of undergrad through the present. I always looked forward to going to Boston, even in the middle of winter, to see all of them and get a chance to hang out again. The friendships really are what I miss most about Boston.

My family has provided huge amounts of love and support throughout the entire Ph.D. process (and my life). My sisters and their families – Laura, Cheryl, Gary, Mitch, Isaac, and Mark – have always been there for me. My Mom has been an incredible role model and has given me an incredible amount of advice, both personal and professional. My father is the one who introduced me to the beauty and the wonder of space, and has of course also been an incredible role model. Both of my parents have been an inspiration to me, and I could not be more proud to be their daughter.

Finally, I need to thank Al. He has pushed me to continue, helped me through tough times with the research, and made me laugh whenever I most needed it. He is my best friend, my rock, the love of my life, and the best husband anyone could ever ask for. Thank you babe.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1

INTRODUCTION AND MOTIVATION

1.1 Motivation

There is a clear need to conduct architectural trades early in the lifetime of a mission to identify those designs that best meet the needs of stakeholders. Typically, these architectural trades evaluate mission performance as a function of a set of design parameters that are assumed to be invariant over the lifetime of a mission. In reality, for many aerospace systems, degrading failures and emergent properties alter system parameters during the course of a mission, thus impacting overall system performance and efficiency. As systems become more complex, engineering judgment is no longer sufficient to understand how the failures of different components in the system, at different points in time, will affect the total system performance. Thus, to complete an accurate risk assessment, it is important to bring together the fields of system performance modeling and reliability modeling in order to model these effects and determine the overall expected system performance, which can then be used in architectural trade studies.

As a result of heritage to techniques used in the nuclear industry [Apostolakis & Michal, 2000], risk assessment in the aerospace industry is almost always purely reliability based. Risk is calculated as the probability of a failure occurring before the end of the lifetime. This type of assessment makes an enormous amount of sense for a safety-critical system, such as any system in the nuclear industry or any manned space flight system. In safety-critical systems the impact of a critical failure at any point in the mission lifetime is the same – loss of human life and mission failure. For non safety-critical systems, such as unmanned missions, the impact of a critical failure depends on when the failure occurs. For most unmanned missions, a critical failure that occurs at the

very *end* of the mission results in the successful return of the majority of data and therefore nearly complete mission success. A critical failure that occurs at the very *beginning* of the mission results in little to no scientific data being returned and therefore nearly complete mission failure. This difference between the impacts of failures depending on when the failure occurs is ignored using current risk assessment techniques, such as Probabilistic Risk Assessment (PRA) [Paulos, 2005]. The definition of risk is the combination of the probability of a negative event occurring and the impact of that event. Therefore, these current risk assessment techniques are actually pure reliability analyses, and not risk analyses, since varying impacts are not considered for non safety-critical systems. While many current risk assessment techniques are answering the question "What is the probability of failure by the end of life?," the true question that needs to be answered for unmanned missions is "How much return, scientific or otherwise, can be expected by the end of the mission design lifetime?" It has been shown that depending on which question is answered, the relative ranking of multiple risk items may be different – leading to different risk mitigation investment decisions. Consequently, the capability to model the probabilistic nature of the expected value of the total system productivity, accounting for the possibility of failures throughout time, is needed. Throughout this report the expected value of the system productivity is called the expected productivity.

In addition to being one of the only risk assessment techniques that truly accounts for all aspects of both probability and impact, expected productivity analysis has many other advantages over current risk assessment techniques. During the design process, risk is often mentioned, but infrequently actually impacts major design decisions. Throughout this discussion a design decision is a decision regarding any level of the design process, from detailed component level decisions to high-level architectural level decisions. One of the main reasons why risk infrequently impacts major design decisions is that risk is considered a qualitative parameter. One design may be judged as "high" risk while another is judged to be "medium" risk, but since a design team member or engineer does not have a clear understanding of what that means, those risk levels rarely impact the choice of one design over another. To be effectively used as a parameter to search a trade-space and make design decisions, it is important to bring risk into the

design process as a quantitative parameter that engineers can understand and trade. One parameter that is almost always used when making design decisions is the productivity of a design. The productivity metric will vary from mission to mission, such as the number of star systems imaged for observatories, or the number of rocks tested for in-situ Mars missions, but it is always a parameter that directly represents to the engineers how well the design is matching the requirements and scientific goals of the mission. If instead of using simple productivity it were possible to examine the expected value of the productivity, defined as the expected productivity, taking into account failures and risk items, the concept of risk could be brought into the design process in a very quantitative way. The engineers could then judge one design from another based on the *expected* number of rocks each will test or the *expected* number of stellar systems each will observe. This would turn risk into a parameter that is not only quantitative, but also one that engineers and design team members can inherently understand and trade.

In addition to risk being considered a qualitative parameter, risk assessment in the early phases of a mission is often considered unnecessary. In the aerospace industry, it is too often assumed that not using risk analysis to facilitate design decisions in the early phases of design is acceptable because a failure of any kind will automatically lead to a complete system failure and the failure of the whole mission. While some effort is given to minimizing these failures or risks through additional testing or added redundancy to critical systems, these efforts are all carried out at the end of the design process. The nearly finalized design is examined for weakness and critical single-point failures and these concerns are addressed late in the design process. Any failure that does not lead to the loss of the mission is considered too unlikely of a scenario to be considered in the early design phase of the mission. Failures that result in reduced productivity but not a complete loss of the mission, known as degraded state failures, do occur on spaceflight systems however, and are more common among these systems than most engineers perceive. A relatively small effort to evaluate degraded states and partial failures during the early phases of the design process could lead to missions that are designed to degrade gracefully. Design decisions can and should be affected by the inherent risk or susceptibility to failures that one design, architecture, or resource allocation strategy has over another, including the ability or inability to degrade gracefully.

Several past missions have benefited from a failure resulting in a degraded state as opposed to a complete system failure. As discussed above, these types of failures are often seen as too unlikely of a scenario to plan for during the early design phases; however, the following examples show that they do occur and are worth considering.

One of the most famous and widely recognized degraded state failures occurred on the Galileo spacecraft en-route to Jupiter. Galileo, launched on October 18, 1989, was an orbiter mission to Jupiter. After the first Earth fly-by on the way to Jupiter, the mission team attempted to open the high-gain antenna that was meant to relay scientific information and engineering telemetry from deep space back to the scientists on Earth. Unexpected friction in several of the ribs caused the antenna to deploy only partially, causing a complete failure of the high-gain antenna. [JPL, Galileo, 2005] Many engineers would have assumed that the complete loss of the high-gain antenna would have resulted in a complete mission failure, since the high-gain antenna is the principle route for receiving science data. In light of the failure, however, mission engineers worked to develop new flight and ground software and NASA's Deep Space Network (DSN) was enhanced to allow science data to be returned at a lower rate through the low-gain antenna. All primary mission data was returned and the mission has been considered a great success. It should be noted that while it was possible to save the mission after this failure, it did take the mission engineers three years to fully restore the communications capability. If a contingency plan for a high-gain antenna failure had been developed, this down time could have been dramatically reduced. Nonetheless, the team was able to return the mission to almost complete functionality, even after a major failure.

A second, more recent, example of what appeared to be a catastrophic failure, that eventually led to the completion of almost all minimum-mission requirements, occurred on September 8, 2004, when the Genesis solar sample return capsule crashed into the Utah desert. Genesis collected solar wind samples for three years and was returning those samples to Earth. The parachutes on the sample canister did not deploy and the canister impacted the Earth at 311 kilometers per hour. The container was breached and the capsule buried into the ground. Contingency planning had laid forth exact procedures

and plans for how to deal with the samples in this situation. The capsule was recovered quickly and moved to a clean room, reducing the risk of further contamination. According to NASA officials, nearly 100% of the mission samples were recovered and the science team believes it will be able to complete nearly all of the primary science objectives [JPL, Genesis, 2005].

Neither the Galileo nor Genesis missions were designed to function under the failure conditions that occurred. In fact, it is unclear if any design improvements could have, or should have, been built into the mission designs to account for these scenarios. Both of these cases, however, show that scenarios in which a major failure occurs can still be very valuable as long as science and mission data are still salvageable. In both cases what initially appeared to be a mission failure, a loss of millions of dollars, and a public relations disaster for NASA, turned into a significant amount of scientific value and a public perception of a mission success with an anomaly. While it is too early to judge how Genesis will be perceived by NASA management and the public in the future, years after the failure on the Galileo mission this near disaster is often completely overlooked when discussing this historic mission and all that it accomplished, and Galileo is often given as an example of one of the great NASA missions.

In addition to the historical examples of missions that have resulted in degraded states, it is clear that as future systems become more complex, the possibility for degraded states increases. Examples of this include distributed and modular systems. The nature of these types of systems will lead to many more degraded, yet highly functional, states. While every mission team would hate to see any kind of anomaly occur on their mission, these examples show the power of partial functionality and degraded states, and provide excellent motivation for ensuring that, within reason and within the scope of other trades, graceful degradation should play a role in design decisions.

While the previous discussion has shown many strong benefits to using expected productivity as a risk metric, for specific types of systems the calculations involved can be complicated. In previous expected productivity modeling work [Wertz, 2002], the productivity of the system depended only on the current functional state of the system.

The productivity was neither time nor path dependent. The functional state of the system itself can often be assumed to be dependant only on the previous state of the system, making it possible to calculate the probability of being in each functional state through time using straightforward Markov models and analysis [Wertz, 2002]. With the additional restriction that the productivity be neither time nor path-dependant, the expected productivity can be calculated as the constant productivity in each state multiplied by the probability of being in that state throughout time and summed over all times and states. While assuming the productivity is path-independent greatly simplifies calculations, it is an invalid assumption for many real life systems. As an example, for this to hold true for observatories, all stars would need to take the same amount of time to observe, and therefore need to be the same in terms of all stellar parameters, including brightness and distance from the Earth. In reality, the stars that TPF-I will observe will vary and will have a wide range of values for stellar parameters such as distance from Earth and brightness. Therefore, the time it takes to survey or observe a particular star system will depend not only on the state of the instrument, but also on the particular characteristics of the star system. This same path-dependant productivity situation is true for any system that is acting on a list of objects or actions that vary in some way and will therefore vary in the time required to complete each.

Nearly all space missions have path-dependant productivities. The time required to take a sample of a rock will depend on the material properties of the rock, and the time required to send a transmission will depend on the size and complexity of the data. Therefore, it is not valid to multiply a constant productivity value for each state by the probability that the system is in that state for each time-step. Instead, the productivity in each state depends on which action in the list the system is executing at that time, which, in turn, depends on the amount of time the previous actions took, and therefore depends on the previous states of the system. The system itself is still a Markov system, since the current state of the system depends only on the previous state. The productivity, however, is now time and path-dependent, making the calculation of the expected productivity much more complicated.

While Monte Carlo simulations can capture the effect of path-dependant productivities, these simulations take a long time to run and are very inefficient, especially when utilizing complicated performance functions. This inefficiency is particularly harmful when broad architecture trade-spaces are being explored and the number of designs to be analyzed is very large. Thus, a more time and effort saving approach would improve both the accuracy and efficiency of these modeling efforts.

1.2 Background and Literature Search

1.2.1 State of the Art

While the previous section discussed the benefits and complications of using expected productivity analysis as a risk tool, this section will discuss the state-of-the-art methods of risk analysis in the aerospace industry, as well as other current research areas in the field of risk analysis. The state-of-the-art risk processes for the aerospace industry can be broken into two main categories – qualitative continuous risk management and quantitative risk analysis. Continuous Risk Management (CRM) involves collecting, monitoring, and controlling the risks that face a program or project in a qualitative way [JPL, 2003]. According to the NASA Procedures and Guidelines, NPG 7120.5B, NASA programs and projects should use the following guideline:

- "The Program or Project Manager applies continuous risk management principles as a decision making tool which enables programmatic and technical success. Decisions are supported by a disciplined process, including the identification, assessment, mitigation, and disposition of risks throughout the life cycle. The entire team assesses risk early in formulation, and throughout the life cycle." [JPL, 2003]

Risk management involves six steps – identify, analyze, plan, track, control, and document and communicate. The process involved in all six steps is to be documented in the Risk Management Plan. Risks are identified and captured on a risk information sheet

and kept in a risk database. Multiple methods are provided by the JPL Project Risk Management Workshop to identify potential risks including checklists, lessons learned databases, fault tree analyses, failure modes and effects analyses, or probabilistic risk assessment. Once identified, risks can be analyzed. Analysis involves assigning either qualitative or quantitative values to the probability and impact of each risk item. For CRM, NASA focuses on a five-level qualitative analysis – very high, high, moderate, low, and very low. The combination of probability and impact leads to fever charts to identify those risks that are most important. Once analysis is complete, the process of planning begins. Planning activities include assigning responsibility, determining the approach, and defining the scope and actions required for each risk item. This may include assigning reserves or margins to resources, adding redundancy, or continued study among other options. Tracking the risk items then involves collecting the planned activities, evaluating the activities and their results, and reporting on the status. Finally, controlling the risks involves the overall execution of the risk mitigation plan and evaluating the results gathered in the tracking stage [JPL, 2003].

In addition to qualitative risk assessment, there are some state-of-the-art quantitative methods of risk analysis used in the aerospace industry. For NASA, the state-of-the-art quantitative risk analysis process is Probabilistic Risk Assessment (PRA). According to Todd Paulos, a PRA expert with the Jet Propulsion Laboratory (JPL), PRA is:

- "A structured, disciplined approach to analyzing system risk.
- An investigation into the responses of a system to perturbations or deviations from its normal operation or environment.
- ...A system simulation of how a system acts when something goes wrong." [Paulos, 2005]

A PRA is basically a quantifiable fault tree and event tree analysis. The systems engineer identifies major events that could affect the state of the system. These events are then placed in an event tree. Following each path through the event tree produces one

sequence of events and results in one of a set of pre-determined end-states. The most common end-states are "ok" and "failed." While other end states can be included, each sequence needs to be laid out and assigned an end state, so a large number of end-state possibilities will lead to a very complicated and tedious analysis. The next step is to create fault trees for each event. These fault trees combine basic events using "and/or" gates among other logic to find the probability of each event in the event tree occurring. The probability of each end-state occurring can then be calculated by working through the logic in the fault and event trees and using the probabilities of the basic events (i.e. the probability of a failure of a given component). Those sequences of basic events that have the largest impact on the total probability of failure can then be identified. This method of quantitative risk analysis is used in the nuclear industry, and has been used at NASA since the Apollo program. Inconsistencies between the predicted probability of success values and the actual percentage of successful missions during the Apollo era made the PRA approach unpopular with NASA engineers and managers, however, and the approach was not used again in the NASA main-stream for several years. The Challenger accident brought PRA back into the forefront however, and at least 13 major PRA studies were conducted at NASA between 1987 and 1995 [Paulos, 2005]. Currently, the NASA policy states that a full scope PRA is required for all missions with a planetary protection requirement, such as sample returns, all missions with nuclear payloads, all human space flight missions, all missions of high strategic importance, including any mission in the Mars program, and all missions with high schedule criticality. In addition, a limited scope PRA is required for any mission costing over $100M and is recommended for all missions [Stamatelatos, 2002].

1.2.2 Current Research Efforts

Ongoing research efforts are continuously searching for ways to improve risk analysis, both in the aerospace and other industries. These research efforts can be categorized into six general categories: identifying risks, estimating and quantifying risk values, uncertainty management, risk analysis case studies, improvements to the PRA process, and the field of performability.

One of the more difficult aspects of risk analysis has always been identifying the full list of risks that affect a given program. Multiple efforts are ongoing to address this difficulty. Tumer, Stone, and Arunajadai are working on approaches and databases to map failure mode identification to the functional breakdown of a particular system. Since it is difficult to identify and estimate failure modes early in the process, when the design is not complete, Tumer et al. feel that by decomposing problems into their functional basis, a more accurate estimate of the failure modes can be obtained even without a complete design [Tumer & Stone, 2001] [Arunajadai et al, 2002]. Additional work is being carried out to identify risks in the conceptual design phase in a concurrent design environment. Meshkat and Scherbenski are currently designing, implementing, and testing risk software and processes to be used in concurrent design environments, such as JPL's Team X. State-of-the-art tools and processes are combined in order to achieve a complete and accurate risk model of a conceptual system. This process has been tested on a case study of a Mars Sample Return mission [Meshkat & Scherbenski, 2005].

Once failure modes are identified, the next step in any quantitative risk analysis process is to estimate the values associated with each risk. Roberts has developed procedures to accomplish just that. Roberts' process involves identifying all risk items, using qualitative measures to first rank the risk items, and then quantitatively analyze the most important risks. The most common method of estimating probability and impact values for risk items is to use historical analogies and databases. Roberts has applied this process to technical, programmatic, schedule, and cost risks [Roberts, 2001]. Wilhite et al. have carried out additional research to quantify the risks associated with technology development. This is a particularly difficult area to estimate in terms of risks given the uncertainty in the nature of technology development. Wilhite et al. have developed both a database tool to collect risks for use in historical analogies, and a tool for assessing the impact of a failure in a technology development area on a program [Wilhite et al, 2003].

One important aspect of risk analysis is uncertainty management and propagation. Uncertainty propagation is a very common method of determining a program's cost or schedule risk. Additionally, uncertainty propagation in terms of technical design parameters can lead to a robust design. It is important to distinguish between a robust

design and a design with reduced risk. Uncertainty analysis in terms of technical variables leads to a design that is able to perform even in uncertain conditions. In other words, a robust design is robust to uncertainty in the nominal conditions of the mission. A low risk design is robust to failures, and deals with the impact and likelihood of off-nominal conditions occurring. An uncertainty in what the nominal conditions are leads to one of many ways in which off-nominal conditions could occur. Therefore, uncertainty propagation of technical variables leads to a single, important risk factor that is then used in the risk analysis. DeLaurentis and Mavris have provided a new method for modeling the technical uncertainty in a design. This method is both explained and demonstrated, using a supersonic transport case study in DeLaurentis, et al. [DeLaurentis & Mavris, 2000] Additional work both in propagating uncertainty and in visualizing the results of uncertainty propagations has been carried out by Walton and Hastings [Walton & Hastings, 2001]. Finally, Hassan and Crossley have used uncertainty propagation to allow the reliability values of components to be random variables in a reliability study of a communications satellite system [Hassan & Crossley, 2003].

In the early design phases, risk is often considered a qualitative variable. However, some work has been done to do early, large-scale, quantitative risk studies of conceptual designs for use in design trade-offs and decisions. An example of this is the reliability-based analysis done by Ebbeler, Aaron, Fox, and Walker for the Space Interferometry Mission (SIM). An Excel-based Monte Carlo tool was used to analyze several different designs for the SIM mission from a reliability standpoint. The study used a complex model of the SIM mission and focused in on the components that were different between designs, as well as those components that made the largest difference from a reliability standpoint. A large amount of effort went into capturing and modeling dependencies in the design and in the failures. While some effort was placed on examining the expected science return from various designs, using a constant productivity rate, the focus of the study was on reliability, or probability of failure. It should be noted that in the conclusions of the study the authors state, "It would be desirable to extend this analysis to compare expected science returns for the competing designs over the nominal 5.5 year mission." [Ebbeler et al, 2003]

The state-of-the-art at NASA for risk assessment in the later design phases is to complete a Probabilistic Risk Assessment, or PRA. The PRA approach has several downsides, however, and multiple efforts are ongoing to attempt to improve the PRA methodology. PRA was developed to determine the probability of failure by the end of a given time, with no consideration for the dynamic aspects of the system. This is the main drawback to using PRA in the aerospace industry and improvements to the PRA process to include this dynamic aspect are ongoing. While the dynamic aspect of systems is particularly important to the aerospace industry, researchers in the other industries have determined a need to include dynamic aspects in the PRAs analyzing nuclear systems as well. PRA is an approach to calculating a final probability of failure, and relies on component probabilities of failure and event probabilities to be accurate. Removing the dynamic elements of any engineering system makes determining the probabilities of these base events more difficult.

As an example, in a nuclear system, a failure occurs only if a chain of events occurs. Several of these events may involve human interaction or even human error. How a human will respond, and therefore the human's probability of error, will depend on past events. If a human operator has made a particular error in the past, he or she is less likely to make that error again. If an action is repeated many times and the operator gets accustomed to completing the action in a given way and then the previous chain of events changes, such that the operator's action should change, the operator is more likely to make an error and revert to his or her usual action. These types of dynamic responses are not captured in a traditional PRA since no aspect of time is considered and therefore there are no conditional probabilities based on the previous set of actions or events.

Several approaches have been developed to deal with these dynamic issues [Siu, 1994] [Devooght & Smidts, 1996] [Cojazzi, 1996]. One of the main approaches for dealing with the dynamic aspect of systems is a phased mission system analysis and phase-modular fault tree, developed by Meshkat, Xing, Donohue, and Ou. In the traditional PRA approach, static fault trees, in which timing aspects are not considered, are used to determine the final probability of failure. In phase-modular fault trees, a fault tree is broken into independent modules. Each module is then solved using either

traditional static fault tree approaches or dynamic Markov chain approaches. Markov chains allow the analyst to consider dynamic aspects to the system. In addition to requiring both static and dynamic fault trees, a phased mission system has multiple phases in which the physical characteristics or requirements for the system might change. As an example, a Mars lander may have launch, cruise, entry descent and landing, and ground phases. In each of these phases the requirements of the system, as well as the systems physical attributes may be different. While some failure rates may change from one phase to another, others may be dependant and linked to a previous phase. This dependency is accounted for in phased mission system analysis [Meshkat et al, 2003]. One way of improving phase-modular fault trees may be to include Semi-Markov chains in addition to Markov chains. Semi-Markov chains allow for additional time to be added for the transition from state to state [Chhikara et al, 2003].

Each of the approaches listed above, while making significant improvements to the traditional PRA approach, still deal exclusively with the probability of failure by the end of a given time. While this captures one extremely important aspect of risk, it often ignores, or does not completely capture, the other aspect – impact. In the aerospace industry, the impact of a failure can vary both by when the failure occurs, as well as by what state the system is left in after the failure. Degraded states, in which performance is lower than nominal but not zero, are possible in the aerospace industry. In addition, if a failure occurs late in life then the productive return of the mission could still be very high if the mission is a non-safety-critical system, such as an unmanned space flight mission.

The computer science and software engineering industries have similar systems that can have degraded states and in which the timing of failures is important. To account for these systems, Meyer has developed a new area of study, known as performability, which combines reliability and performance analyses [Meyer, 1980]. Performability combines Markov, or Semi-Markov, chain analyses with a performance level in each state, to determine the overall system performance. The metric in most performability analyses is the probability that the system will meet a given performance requirement. This is a slightly different metric than the previously proposed expected value of the performance, or expected performance. Additionally, all performability

analyses found to date have used a constant performance value for each state of the system [Ciardo et al, 1990] [Smith et al, 1988] [Meyer, 1980]. Therefore, these analysis methods would not be applicable to systems with path-dependant productivities.

While the majority of performability analyses have been done on software or processor systems, Ciciani and Grassi have completed a performability analysis of a fault-tolerant commercial satellite system. This performability analysis again used the probability that the system will meet a given performance as the metric, as well as constant productivities in each state. The analysis was done on a small portion of the satellite system, specifically the number of transponders that should be included in the full system. All subsystems other than the communications subsystem were given a common, single failure rate. Therefore, while this study was a large step in the direction of using the expected value of the performance as a risk metric for aerospace systems, it was limited in the type of system it could analyze (no path-dependant systems), and in the level and number of design decisions that could be affected (number of transponders). This study did, however, set the precedent that a metric that combines both the performance and the reliability into a single metric is needed to achieve a full risk analysis of an aerospace system [Ciciani & Vincenzo, 1987].

Jilla and Wertz performed the first studies on aerospace systems in which the expected value of the performance metric was used as a figure of merit. These studies introduced the concept of combining reliability and performance into a single metric for use in design trade studies. While they laid the initial groundwork for the research developed in this document, the focus of these studies was on system modeling and trade tool development, and not on risk analysis. Additionally, none of the previous studies that involved expected productivity included the ability to analyze systems with path-dependant productivity functions [Wertz, 2002] [Jilla, 2002].

1.3 Research Objectives and Approach

1.3.1 Objectives

The first primary objective of this research is to develop a new risk metric for use with non safety-critical systems in the aerospace industry, along with a methodology for analyzing this metric. This new risk metric needs to cover two additional objectives – capturing all aspects of risk for non safety-critical systems, including varying impacts, and facilitating the use of risk as a design decision parameter in the conceptual design stages. It is important to develop the methodologies and techniques needed to accurately and efficiently model all components of risk for non safety-critical systems. This includes the ability to model the varying impacts of failures occurring at different points in time in the lifetime of the mission. Additionally, it is important to capture failure modes that lead to degraded states instead of complete mission failure. Capturing all components of risk accurately is only useful if the associated risk metric actually influences design decisions. Since design decisions made in the early stages of design have the largest impact on the overall performance, cost, and risk of the final product, it is additionally important that the risk metric developed be easily applied to missions in all stages of design, including conceptual design.

In order to meet all the objectives listed above, a risk metric of expected productivity has been proposed. The expected productivity of a system is the product of the probability of being in each functional state and the productivity in that state, summed over all states and all time. Calculating the expected productivity of a system is relatively simple if the system productivity depends only on the functional state of the system. If the system productivity is additionally path-dependant, the complexity of the calculation of the expected productivity for the system is greatly increased. Therefore, a second objective of this research is to develop a modeling methodology to efficiently and accurately estimate the expected productivity over a given lifetime of systems with path-dependant productivities.

The third primary goal of this research is to show, through case studies using a real mission, that risk can be analyzed and can affect design decisions in the early design

stages. The application mission for this research, TPF-I, is in a very early design stage. In addition, mitigating perceived mission risk is considered to be a top priority for the TPF-I design team. Therefore, a secondary objective of this research is to work with the TPF-I design team to bring failures and risks into the design process.

The primary and secondary objectives of this research are shown below.

- Develop a new risk metric for use with non safety-critical systems in the aerospace industry. Ensure that the given risk metric:
  - Captures all aspects of risk for non safety-critical systems, including varying impacts.
  - Facilitates the use of risk as a design decision parameter in the conceptual design stages.
- Develop a modeling methodology to efficiently and accurately estimate the expected productivity over a given lifetime of systems with path-dependant productivities.
- Show through case studies, using a real mission, how risk can be used early in the design process.
  - Work with the TPF-I design team to bring failures and risks into the design process.

1.3.2 Hypothesis

This research is based on the hypothesis that a change in the method of how risk is represented will lead to risk becoming a factor in early design phase decisions. It is assumed that if risk is presented as expected productivity, which designers can understand and assign value to, it will become a factor in design decisions. It is also assumed that some knowledge about the failure modes and probabilities of failure for a design is known in the early design phases. This knowledge can be based on pure

engineering judgment, but a basic knowledge is required. Finally, it is assumed that missions in the early design phases have a system model capable of calculating the system level productivity, and that the model can be modified to include degraded states. This system model should be appropriate for the phase of the design process, and can therefore have various levels of fidelity.

1.3.3 Approach

An approach has been developed to model the expected productivity of systems with path-dependant productivities in a more efficient and effort saving manner than a Monte Carlo simulation. The basic principle behind the approach is to find the expected path and then find the expected productivity given the expected path. The seven main steps to this approach can be seen in Figure 1-1. Note that while Figure 1-1 shows the basic principles behind the steps to the modeling approach, there are many details and adjustments that need to be made before implementing the approach. The approach, called Expected Productivity Risk Assessment (EPRA), is covered in more detail in later chapters of this report.

1. **Use probability of failures prior to operations to determine the initial conditions and the expected value of the initial system performance variables**
2. **Use Markov modeling to find *P*, the probability of being in each state at each time-step**
3. **For each object*, based on the probability of being in each state at the beginning of that object and the time required in each state, find the expected number of time steps to complete the object**
    1. Normalize probabilities based on only those states in which completing the object is possible
4. **Calculate a vector of the probabilities of being in a functioning state at the time each object is expected to be completed**
5. **Based on the expected time to complete each object and the probability of being in a working state at that time, find the vector of probabilities that the system completed exactly each number of objects before failing.**
6. **Determine expected productivity and standard deviation**
7. **Find the probability of completing each number of objects or less, or the Cumulative Distribution Function (CDF)**

*** An "object" is defined as a single unit of the performance metric. Examples include an image for an observatory, or a measurement for an instrument.**

Figure 1-1: Basic steps to the Expected Productivity Risk Analysis (EPRA) approach.

1.3.4 Case Studies

The concepts of expected productivity and degraded state analysis have been applied to the Terrestrial Planet Finder Interferometer (TPF-I) mission. The mission is planned for launch in 2020 and is a very complex, formation flown interferometer mission with an objective of finding and characterizing Earth like planets around other stars. Additional details about the TPF-I mission can be found in Chapter 3. The main metric used by TPF-I to date to evaluate one architecture option against another is the number of star systems that the architecture can observe. However, with the exception of the studies associated with this research effort, these star counts did not take into account any failures or off-nominal scenarios. Because of the complexity of formation flown interferometers, missions of this type are perceived to be risky by both management and the general public. One of the major challenges presented to the design teams has been to reduce this perceived risk. If instead of nominal star counts, the design team could calculate the expected star count, taking into account known failure modes and risks, this

metric could be used to represent both the performance and associated risk of an architecture option. If this expected star count is acceptable to reach mission success, the perceived risk of the mission could be dramatically reduced. Therefore, an effort has been on-going to calculate and use the expected star count for the TPF-I mission.

The path-dependant expected productivity analysis approach discussed above has been used to calculate the expected star count for candidate TPF-I architectures. This expected star count, as well as the process of calculating it, have already impacted the design of the TPF-I mission in several ways.

Since the basic design for the TPF-I mission involves several spacecraft in a formation, previous design-team discussions have explored degraded states that could occur if there was a failure of a single spacecraft. Prior to this study, most of these discussions were dismissed with the assumption that if any of the spacecraft were to fail then the mission would certainly be lost. An initial round of analysis has been completed to challenge that assumption. Each of the multiple spacecraft architectures under consideration for TPF-I was examined without each of the possible component spacecraft to determine if interferometry would still be possible. Interferometry, and therefore the observation of a star system, is only possible if the light paths to the combining optics from three or more collecting apertures are equal in length and the phases of these light beams can be summed to zero. It quickly became evident that none of the architectures could function in a degraded state if the phase of the light coming from each of the apertures was fixed and could not be varied if a failure had occurred. However, several of the architectures could still function with the loss of a single spacecraft if these phases were variable.

At the same time that this analysis was being performed, work had already begun on the design of the instrument, including the beam transport and combining system. Given the information about the ability to degrade to partially functional states if the phases of the beams were variable, the design team members began to examine the difficulty of achieving variable phasing. The beam combiner design that had been under development was more difficult to modify to allow for variable phases than a secondary

design which had been examined but not developed in detail. Therefore, the design team members recommended that the baseline beam combining system design be switched, at this early stage of the mission, to allow for the ability to degrade to partially functional states in the event of a single spacecraft failure. If this design decision had not been made at this early point in the design, the difficulty of adding variable phases later would have either pushed the design process over budget or would have been too difficult to accommodate, and degraded states after the loss of a single spacecraft would not be possible in flight. While it is still unclear if the architecture that will eventually be flown for TPF-I will be one that can accommodate a single spacecraft failure, it is clear that the knowledge of what would be required to achieve this graceful degradation has made a positive impact on the design process.

In addition to facilitating design decisions that enable graceful degradation, the same graceful degradation analysis discussed above has also affected architecture design decisions by introducing the level of graceful degradation as a metric used to discriminate between architectures. In December 2004, the TPF-I design and architecture teams participated in a series of meetings intended to score various architectures against one another in order to down-select to a baseline architecture to be considered in more detail during future studies. The architectures were scored for 27 different weighted parameters. The weighted scores were then summed together for each of the architectures in order to compare the overall designs. The weights for all 27 parameters summed to 100, leading to an average weight of 3.7. The ability to degrade gracefully was one of the parameters considered and had an above average weighting of 4.3. The score each of the architectures received in graceful degradation had a significant impact on the overall score, and therefore had a significant impact on the architectural decision arrived at during these meetings. Again, by introducing the concept of graceful degradation and risk at an early stage in the design process, the TPF-I team has been able to make decisions that make risk reduction techniques and lower risk designs a high priority without having a large negative impact on resources at the end of the design cycle.

The final way that risk and reliability are brought into the TPF-I design process at this early stage is through specific design-based risk modeling and analysis. A detailed risk list for the current TPF-I design has been compiled through interviews with experts on the design and architecture teams. Most of these experts initially stated that no real consideration has been given to risks or failures yet. However, through the interview process it was possible to gather information about what each particular expert is concerned about in the design. These concerns translate directly into risks. The current risk list consists of information gathered from interviews from eleven different subsystem experts: the attitude control system (ACS), structures, the autonomous formation flight sensor system (AFF), formation flight algorithms and control, technology development, architecture development, instrument, and four systems experts. These interviews have led to 102 individual failure modes or risk items. For each of these failure modes or risk items, information is gathered on the nature of the risk, the probability of the negative event occurring, and the impact if that event does occur. The impact can range from no impact, if there is a completely redundant system on board, to complete system and mission failure. The impact of a particular risk item or failure can also be a degraded state, where there is some functionality in the system, but some parameters are no longer nominal. These partial failure impacts can include, among others, an increased probability of failure or increased failure rate of a different failure mode or risk item, increased observation time, or reduced observational efficiency. Of the 102 current risk list items, 26 result in a complete system failure, 36 result in a degraded state, and 40 result in either a complete failure or a degraded state depending on the severity of the failure or level of redundancy in the system. While the probability of failure or the failure rate of a particular risk item is often hard to judge at this early stage in the design process, the relative probability of each failure occurring is much more intuitive. Events were binned into those that are very likely to occur, likely to occur, somewhat likely to occur, not likely to occur, and very unlikely to occur. These probability bins were then assigned specific probability values that were later examined in a sensitivity analysis.

Once the probability and impact of each risk item were known, a risk model was developed. Given a particular set of risks and their associated values, the expected productivity of the system was calculated. With all probabilities of failure and impacts

set at the nominal level, the risk model returns an overall expected star-count of nearly 123 stars for the detection phase of the mission. The probability or impact values of different risk items were then altered to model mitigation of those particular risk items. When the model was run again with these adjusted probability or impact values, the expected productivity of the system increased. The difference in the expected productivity of the system with the adjusted values and the original system represents the value gained by the mitigations. In this way, those risk items that have the largest impact on the overall system expected productivity can be identified, and given priority in terms of risk mitigation strategies early in the design process. This provides another method of using risk and reliability analyses in the early design stages to influence both the design and the overall mission and resource allocation strategy.

By using the expected value of the total system productivity to represent risk, it is possible to enable design decisions at an early stage of the design process that incorporate risk modeling considerations. When these design decisions are made earlier in the design process, the cost of these decisions is significantly reduced. The work that has been conducted in this study introduces large strides in the effort to bring risk and reliability into the design process at an earlier phase by introducing these approaches and applying them to an actual mission example using the TPF-I mission.

1.4 Overview of Thesis

The remainder of this document presents the approach developed for calculating the expected productivity of systems with path-dependant productivities and provides case studies as examples of how and why to use this new risk analysis methodology. Chapter 2 covers why expected productivity analysis is a necessary risk assessment technique. Chapter 3 presents the new methodology, called Expected Productivity Risk Analysis (EPRA), for calculating the expected productivity of systems with path-dependant productivities. This chapter includes both the mathematical and conceptual details behind the approach, as well as calibration of EPRA results against Monte Carlo simulation results. Chapter 4 gives an overview of the application mission for this

research, TPF-I. This chapter also includes a brief introduction to the concept of interferometry and a brief description of the main productivity model being used by the TPF-I design team. Chapters 5 and 6 present the two case studies highlighting how risk, when represented by expected productivity, can be incorporated into the design process at an early stage of the design. The first case study, presented in Chapter 5, compares multiple architectures under consideration for TPF-I from a graceful degradation standpoint. The second case study, presented in Chapter 6, examines the risks inherent in the current TPF-I architecture and analyzes those risks. The final chapter, Chapter 7, summarizes the conclusions of this research, the contributions that have been made, and the suggestions for future work in this arena.

Chapter 2

EXPECTED PRODUCTIVITY AS A RISK ASSESSMENT TOOL

2.1 Expected Productivity

The definition of risk is the combination of the probability of a negative event occurring and the impact of that negative event. Therefore, risk assessment needs to incorporate both the probability of a failure occurring and the impact of that failure. When dealing with safety-critical systems the only important failures are critical failures, and these all result in the same impact – loss of human life. With non safety-critical systems, however, the impacts of failures are more varied. The timing of when a failure occurs affects the impact on the overall mission performance. Additionally, failures that result in lowered performance, but not complete mission failure should be modeled to determine the impact. The expected value of the overall productivity of a system, or the sum of the products of the possible productivities in various states multiplied by the probability of those states occurring, takes into account all aspects of true risk assessment since both probabilities and impacts are considered. This type of assessment is defined as expected productivity analysis.

As discussed in Chapter 1, expected productivity analysis has many benefits in terms of use as a risk metric. The largest benefit however, is the natural fit of how well the expected productivity represents the true meaning of risk. By definition, the expected value of a variable is the probability of a value occurring multiplied by the specific value. This is basically identical to the definition of risk – the probability of a particular event occurring times the impact of that event. When dealing with non-safety-critical systems the impact of a given event is best measured by the productivity of the state that remains

after the event. Therefore, a natural choice for a risk metric is the expected value of the productivity of the system, or the expected productivity.

2.2 Differences Between Traditional Risk Assessment Techniques and Expected Productivity Risk Assessment Techniques

As discussed in Chapter 1, traditional risk assessment techniques are different from expected productivity risk assessment in terms of the question that is being answered. In traditional risk assessment techniques, the question is what is the probability of a critical failure by the end of the mission lifetime? In expected productivity risk assessment techniques, the question is how much return can be expected from the system? Each risk assessment technique will not only determine the answer to the associated question, but will also rank how much each risk item being modeled has affected that answer. The more a risk item affects the overall answer, the more important that risk item is to the project or program. This is measured using one or more importance measures. The higher the importance measure of a particular risk item, the more impact it has on the overall risk of the system, and therefore more resources should be committed to mitigating or controlling it. Independent of which question is answered, or which risk metric is used, the ranking of the risk items should be comparable between the various importance metrics, in terms of the impact to the overall risk of the project or program. If different risk metrics lead to the same ranking of the risk items then the results using the different metrics would lead to similar courses of action by management and decision makers. If rankings are significantly different using different risk metrics, then the resulting courses of action that a program or project will take would most likely vary.

For a very simple example problem, three main importance measures that use overall probability of failure as a risk metric will be compared to a new importance measure that uses expected productivity as a risk metric in order to highlight the differences between the two. The three importance measures that use probability of

failure as a risk metric are the Birnbaum and Fussell-Veseley importance measures and the percentage of the total probability of failure from a given set of events.

Birnbaum was the first to introduce the concept of an importance measure to reliability analysis. This importance measure calculates the sensitivity of the total probability of failure to the probability of a particular event or risk item. The equation for the Birnbaum importance measure is given below [Wang et al, 2004] [Hoyland & Rausand, 1994].

$$I_{Birnbaum}(A) = \frac{\partial P_{Failure}(total)}{\partial P_A} \qquad (2\text{-}1)$$

Here $I_{Birnbaum}$ is the Birnbaum importance measure, A is the risk item or event of interest, $P_{Failure}(total)$ is the total probability of failure, and P_A is the probability of event A occurring. While Equation 2-1 is the general form of the Birnbaum importance measure, a different form is often used to ease calculations. The general form, as shown in Equation 2-1, is the sensitivity of the total probability of failure to a change in the probability of the event of interest. The form of the equation is greatly simplified if the change in the probability of the event is set equal to 1. In this case the denominator of Equation 2-1 is simply 1 and the numerator is the difference in the system probability of failure with the probability of the event of interest set to 1 and 0. This form of the Birnbaum equation is given in Equation 2-2 and is used in the examples that follow in this section [Smith et al, 2002] [Relex, 2005].

$$I_{Birnbaum}(A) = \left(P_{Failure}(total) \middle| P_A = 1\right) - \left(P_{Failure}(total) \middle| P_A = 0\right) \qquad (2\text{-}2)$$

The final two importance measures discussed here that use probability of failure as a risk metric both use the idea of minimal cut-sets. A cut-set is a particular path through a system, or set of events, which will lead to system failure. A minimal cut-set is a cut-set in which if a single event were removed, the system would no longer fail [Paulos, 2005]. In fault-tree analyses, minimal cut-sets are often used to describe the important failure paths of the system. As an example take a system that consists three components: A; B; and C. The system will fail if either component A or one of

components *B* and *C* fail. This system is shown in the fault-tree in Figure 2-1. In this case, the minimal cut-sets are *{A}* and *{BC}*. Note that the set *{ABC}*, while a cut-set, is not a minimal cut-set because if you remove either *B* or *C* from it the system would still fail since *A* is still in the set.

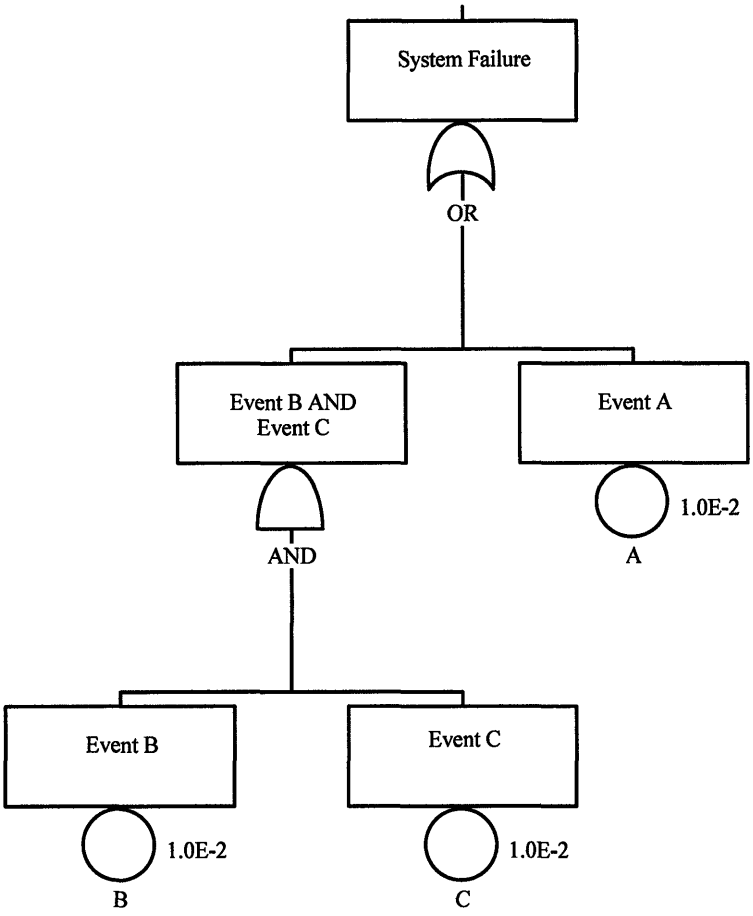


Figure 2-1: Example fault tree - the minimal cut-sets are {A} and {B,C}

The first importance measure that uses the concept of minimal cut-sets is the Fussell-Vesely importance measure. The Fussell-Vesely importance measure calculates the probability of the union of all minimal cut-sets that contain the event of interest divided by the probability of the union of all minimal cut-sets [Relex, 2005]. This is shown below.

$$I_{Fussell-Vesely}(A) = \frac{P\left(\bigcup\{AllCutSetsContainingA\}\right)}{P\left(\bigcup\{AllCutSets\}\right)} x100\% \qquad (2\text{-}3)$$

It may be difficult for software programs to automatically determine all the cut-sets containing the specific event of interest. Since this is required for the numerator of Equation 2-3, it is often useful to put the Fussell-Veseley importance measure in a different form. The probability of the union of all minimal cut-sets containing A can be thought of as the probability of the union of all minimal cut-sets minus the probability of the union of all minimal cut-sets not containing the event A. The latter can be easily found by setting the probability of event A to zero and recalculating the probability of the union of all minimum cut-sets. This form of the Fussell-Veseley importance measure is given below and is used in the examples in the following discussion [Smith et al, 2002] [Wolfram, 2005].

$$I_{Fussell-Vesely}(A) = \frac{P\left(\bigcup\{AllCutSets\}\middle|P(A)=P_A\right) - P\left(\bigcup\{AllCutSets\}\middle|P(A)=0\right)}{P\left(\bigcup\{AllCutSets\}\middle|P(A)=P_A\right)} x100\% \qquad (2\text{-}4)$$

In Equation 2-4, $P(A)$ is the probability of event A occurring and P_A is the original probability of event A occurring.

The final importance measure that uses the probability of failure as a risk metric is the percentage of the total probability of failure from a given cut-set. This metric measures the importance of minimal cut-sets instead of basic events. Both the Birnbaum and Fussell-Veseley importance measures calculate the importance of basic events. If a system consists of only single-point failures the minimal cut-sets and the basic events are identical. The cut-set importance meaure is given below [Smith et al, 2002] [Paulos, 2005].

$$\mathrm{I}_{cut-set}(A) = \left(\frac{P(A)}{P_{Total}(failure)}\right) \times 100\% \qquad (2\text{-}5)$$

Note that A in Equation 2-5 is a cut-set, and not a basic event like in Equation 2-4.

In order to make a comparison to the existing importance measures discussed above, a new importance measure needs to be defined using the expected value as a risk metric. The expected productivity importance measure is modeled after the concepts from both the Fussell-Veseley and Birnbaum importance measures. The impact of an event or risk item is determined by finding the expected productivity of the nominal system, in addition to the expected productivity given a zero probability of the given risk item occurring. Since the negative event would have lowered the expected productivity, the expected productivity should increase when the probability of the event occurring is set to zero. The impact of the event or risk item is then simply the expected productivity with the probability set to zero minus the expected productivity with the probability set to the original value. This is then normalized by the expected productivity with all probabilities set at the original values and turned into a percentage. The equation for the expected productivity importance measure is shown below.

$$I_{EP}(A) = \left(\frac{\left(E[p](P(A) = 0)\right) - \left(E[p]P(A) = P_A\right)}{\left(E[p]P(A) = P_A\right)} \right) \times 100\% \qquad (2\text{-}6)$$

In Equation 2-6, I_{EP} is the expected productivity importance measure, $E[p]$ is the expected productivity, A is the risk item or event of interest, $P(A)$ is the probability of event A occurring used in a given calculation, and P_A is the original input for the probability of event A occurring.

In order to show the differences between using expected productivity versus probability of failure as the risk metric, a simple example problem has been created. For this problem, the system of interest has only two failure modes, both of which are single point failures. The first failure mode is from a deployment. The deployment only occurs once and needs to be completed in order for the system to enter operations. The second failure mode is from a moving component. The component is required once operations begin and can fail at any point throughout operations. If either the deployment or the moving component fails the system is in a failed state. With this system there are two basic events (deployment failure and component failure) and only two minimal cut-sets (deployment failure and component failure). The importance of each of the two events or

cut-sets was calculated using each of the importance measures described above for varying values for the probability of each event occurring. Additionally, the two events were ranked using each importance measure to determine which failure mode is the more critical mode and should have priority in terms of mitigation actions. The results are shown in Figures 2-2 through 2-4.

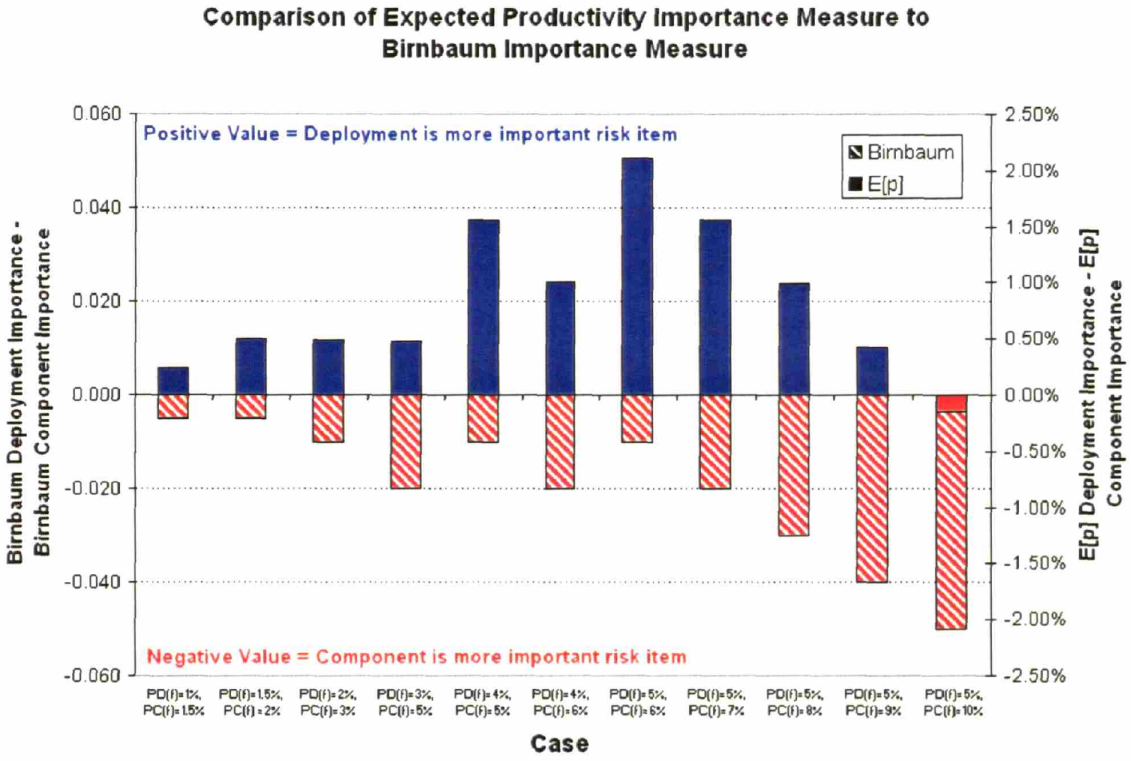


Figure 2-2: Example problem results comparing the Birnbaum importance measure to the expected productivity importance measure

In Figures 2-2 through 2-4, *PD(f)* is the probability of deployment failure and *PC(f)* is the probability of component failure by the end of the lifetime of the mission. An exponential failure rate was assumed for the component failure. The specific values used for the probability of failure are given as the case definition on the x-axis. Note that in all cases the component has a higher probability of failure by the end of life than the deployment probability of failure. The y-axes in all three figures are the importance

measures for the deployment failure minus the importance measures for the component failure. Therefore, a positive value implies that the deployment failure is the more important failure mode. Similarly, a negative value implies that the component failure is the more important failure mode. The first thing to note about all three figures is that in ten of the eleven cases tested the expected productivity importance measure ranked the two failure modes in opposite order from the existing importance measure. In several cases the component failure was measured to be significantly more important than the deployment failure using the existing importance measures, but the expected productivity importance measure finds that the deployment is actually the more important failure mode. These discrepancies mean that using current risk analysis techniques, an engineer or designer would assign more importance and therefore more resources to mitigating the component failure mode. However, if the key metric is actually the expected return of the mission and not the probability of failure by the end of the lifetime, more importance and therefore more resources should be focused on the deployment failure. The reasons for this are clear. The component has a higher probability of failure by the end of the mission lifetime. Therefore, existing measures that use probability of failure as the risk metric rank the component failure mode higher than the deployment failure mode. The component may fail at any point throughout the mission lifetime, however, including only a short time before the scheduled end of the mission. If the component fails after any significant amount of time has passed then the mission will still have returned some useful data. The deployment failure occurs at only one point in time, before operations. If the deployment fails, no data will be returned from the mission. This is not dependant on the timing of the failure since the event must occur before operations even begin. Therefore the deployment actually has a larger impact on the system than the component failure. Since risk, in addition to expected productivity, measures the combination of probability and impact, this higher impact outweighs the lower probability in ten of the eleven cases shown. This effect is not captured with the current risk metrics and importance measures. Note that in all three figures the only case in which both importance measures lead to the same ranking of failure modes, the probability of failure for the component is twice the probability of a deployment failure.

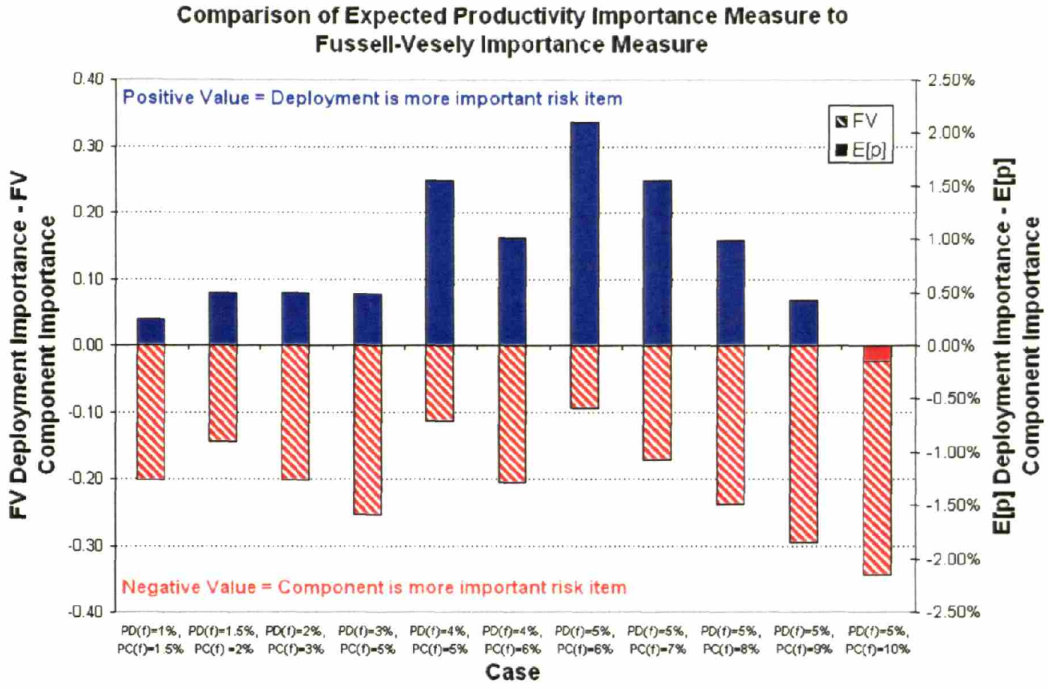


Figure 2-3: Example problem results comparing the Fussell-Veseley importance measure to the expected productivity importance measure

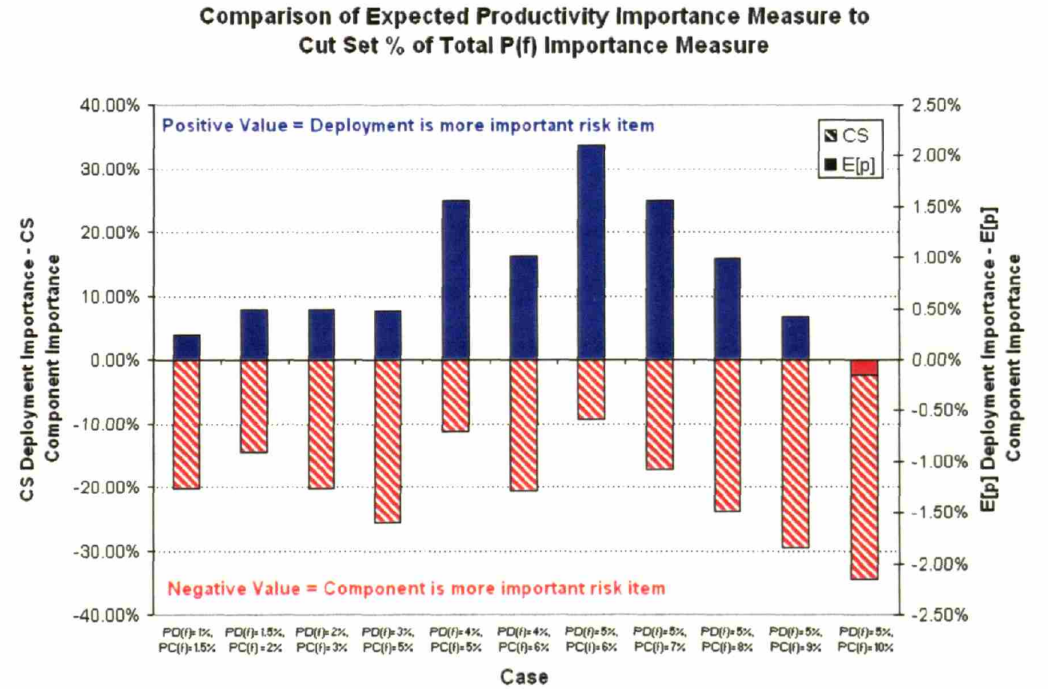


Figure 2-4 : Example problem results comparing the cut-set importance measure to the expected productivity importance measure

A subset of the cases shown in Figure 2-2 are shown in Figure 2-5. In these figures the probability of deployment failure is set at a constant value of 5%. The probability of failure for the component varies along the x-axis from 6% to 10%. This set of cases clearly shows the differences between the importance measures. If the probability of component failure is only slightly higher than that of deployment failure, the current importance measures will indicate that the component failure mode is the most important failure mode but only by a small margin. In contrast, using the expected productivity importance measure, the deployment is ranked as the more important failure mode by a significant margin. As the component probability of failure increases the differences in the importance of the two failure modes increases for the probability of failure importance measure but decreases for the expected productivity importance measure. Note that these same trends, while only shown for the Birnbaum importance measure, occur in Figures 2-3 and 2-4 as well for the Fussell-Veseley and cut-set importance measures.

The previous examples highlight the differences between using probability of failure and using expected productivity as the risk metric in trade studies and risk analyses. Since probability of failure only captures the probability aspect of risk, if the impacts of the failures are significantly different, either due to degraded states or due to the timing of the failures as in the previously discussed examples, importance measures that rank risk items in terms of their impact on the probability of failure can give misleading results. Current risk analysis techniques may lead to resources being allocated inappropriately, such as if more resources were devoted to mitigating the component failure mode over the deployment failure mode in the previous example.

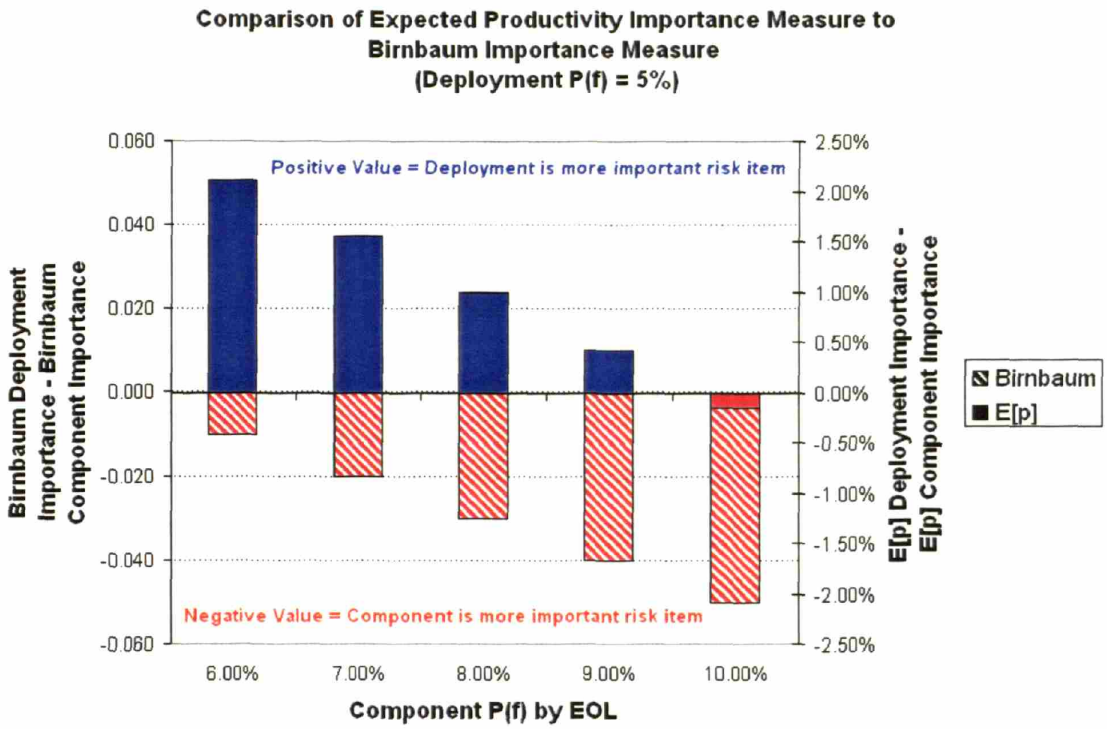


Figure 2-5: Subset of comparisons between the Birnbaum and expected productivity importance measures

2.3 *Complexities of Using Expected Productivity as a Risk Assessment Tool*

2.3.1 Mission Uniqueness

Tools exist to do risk assessment for missions of all varieties. Combining the systems performance aspect with the probabilistic aspect of risk analysis leads to the need for much more customized tools for each individual mission. In the same sense that each mission needs a system performance model that is custom built for that mission, it will also need a risk assessment model that is custom built for that mission (utilizing the already custom built performance model). Engineers running these analyses will need to understand both the system performance and the probabilistic aspect of risk. This challenges conventional thinking and would require engineers to be trained in this new methodology. With more attention paid to educating existing systems engineers in

probabilistic assessment, however, this challenge could be easily met by an engineer in a conventional systems engineering role.

2.3.2 Path-dependant Productivities

As discussed in Section 1.1, calculating expected productivity is relatively simple if the system productivity is dependant only on the functional state of the system. In these cases the expected productivity is simply the productivity in each state multiplied by the probability of being in that state. Many real-life aerospace systems however have productivities that are time or path dependant. An example of this is an observatory system. The time required to examine a particular star depends not only on the functional state of the instrument, but also on the characteristics of the star. Stars that are fainter or further away may take longer to characterize than those that are brighter or closer. The productivity in each state now depends on which object in a given list the system is processing at that time, which in turn depends on the amount of time the previous objects took to process, and therefore depends on the previous states of the system. The system itself is still a Markov system, since the current state of the system depends only on the previous state. The productivity, however, is now path-dependent, making the calculation of the expected productivity much more complicated. An approach to calculating the expected productivity of path-dependant productivity systems has been developed and is discussed in detail in Chapter 3.

Chapter 3

THE EPRA PATH-DEPENDANT PRODUCTIVITY MODELING APPROACH

3.1 Motivation for a New Modeling Methodology

As discussed in Chapters 1 and 2, there are many benefits and advantages to using the expected value of the total system productivity, or the expected productivity, as the metric used to measure the risk of non-safety critical aerospace systems. This chapter presents a new method of calculating the expected productivity for a system in which the nominal productivity is path-dependent.

Calculating expected productivity is relatively simple if the system productivity is dependant only on the functional state of the system. In these cases, the expected productivity is simply the productivity in each state multiplied by the probability of being in that state. Unfortunately, many real-life aerospace systems have productivities that are time or path-dependant. An example of this characteristic is an observatory system. The time required to examine a particular star depends not only on the functional state of the instrument, but also on the characteristics of the star. Stars that are fainter or farther away may take longer to characterize than those that are brighter or closer. For any system of this nature, the productivity in each state depends on which object in a given list of objects the system is processing at that time, which in turn depends on the amount of time spent completing the previous objects on the list, and therefore depends on the previous states of the system. In the observatory example, the list of objects may be a list of observations of specific stars. Other examples include a list of measurements from

specific rocks or sites for an in-situ instrument or a list of traverses of varying distances and difficulties for a rover. The list of objects the system is processing can also represent varying actions, such as different types of measurements on a particular rock. The productivity of the system is measured by the number of objects that are completed in the given lifetime, such as the number of observations or the number of measurements. Note that even for systems with path-dependant productivities, the system itself is still a Markov system, since the current state of the system depends only on the previous state; however, the system productivity is now path-dependent, making the calculation of the expected productivity much more complicated.

Prior to this work, the only method available to calculate the expected productivity of a system with a path-dependant productivity function was to use a Monte Carlo simulation. Monte Carlo simulations are a way of calculating the statistical outcomes of uncertain events using "brute-force." A simulation of the mission is repeated a large number of times, each time with uncertain variables or outcomes given a single value determined by their probability distributions. In the case of expected productivity analysis, each simulation follows a single path through the mission, resulting in one of the many possible outcomes for the total system productivity. Once many simulations have been completed, these different outcomes can be averaged to find the overall expected value of the system productivity, or the expected productivity.

While the Monte Carlo approach is a well understood and trusted approach, it has several draw-backs. Since Monte Carlo simulations require the full productivity to be calculated a large number of times, these simulations can take a very long time to complete. This is especially true if calculating the productivity of the system is complicated and time-consuming for even a single case. If calculating the system productivity for a single case takes several minutes, repeating this process hundreds of times for the Monte Carlo simulation will take hours or even days. If the expected productivity is to be used as a metric to represent risk in a trade-study, this calculation will need to be repeated many times for many different designs. Therefore, if a simulation which takes days to run is required to calculate the expected productivity for a single design, it is unlikely that this metric will actually be used in a trade-study.

Additionally, because a Monte Carlo simulation uses random sampling of uncertain variables, the outcomes are by definition uncertain. While the uncertainty in the results can be reduced by increasing the number of runs per simulation, this uncertainty can never be truly removed. The uncertainty in the results makes sensitivity studies or comparisons between two similar designs very difficult, since it is unknown if small differences in results are due to a change in the design or input parameters, or simply due to variations in the uncertain samplings between the simulations.

A more efficient and more repeatable approach to calculating the expected productivity of systems with path-dependant productivities has been developed. This new approach is called Expected Productivity Risk Analysis (EPRA), and is described in the following sections.

3.2 The EPRA Modeling Approach

The basic concept behind the EPRA approach to modeling the overall expected productivity of a path-dependent system is simple – find the expected path through the system, and then find the expected results given that path. The basic steps to the approach, and the order in which they occur, are shown in Figure 3-1.

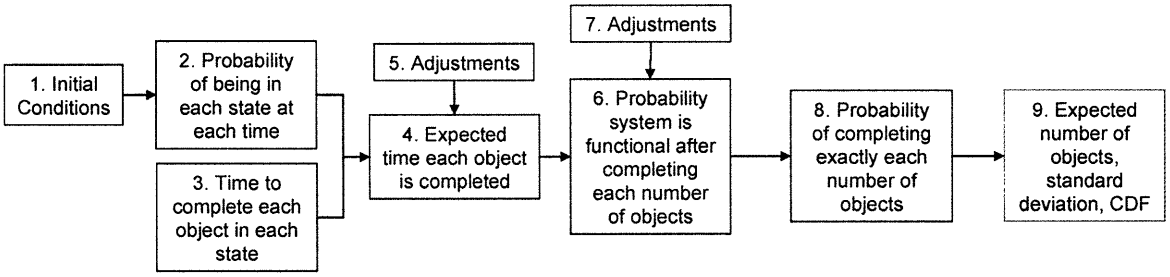


Figure 3-1: Basic approach to the EPRA methodology for modeling the expected productivity of path dependent systems

The first step to the EPRA approach is to determine the initial conditions for the problem. The initial conditions are set by examining any possible failures that would occur prior to the beginning of operations.

Next, the probability of being in each state, at each time, is calculated using Markov modeling. The time to complete each object in each state is calculated using a productivity model. Note that throughout this discussion, an object is defined as a single unit of the performance metric.

Once the probability and productivity information is known, it is possible to calculate the expected amount of time required to complete each object. Prior to this calculation, a few adjustment calculations are required. These adjustments account for specific, often unusual circumstances, and are calculated automatically.

The expected time required to complete each object can then be used to calculate the probability that the system is still functional after completing each number of objects. This calculation will again require some adjustments to account for specific circumstances.

Next, the probability of completing *exactly* each number of objects can be calculated. Given these probabilities, it is relatively simple to calculate the expected number of objects completed, the standard deviation off of this expected value, and the cumulative distribution function (CDF).

Figure 3-1 and the previous discussion give a broad overview of the EPRA approach. Each of the nine basic steps shown in Figure 3-1 will be discussed in detail in the following sections.

3.2.1 Step 1: Determining Initial Conditions from Possible Failures Prior to Operations

The first step in the EPRA approach is to determine the initial conditions for the simulation. The initial conditions are set by the possibility of failures prior to the

beginning of operations. This step is shown and summarized in Figure 3-2, and discussed in detail below.

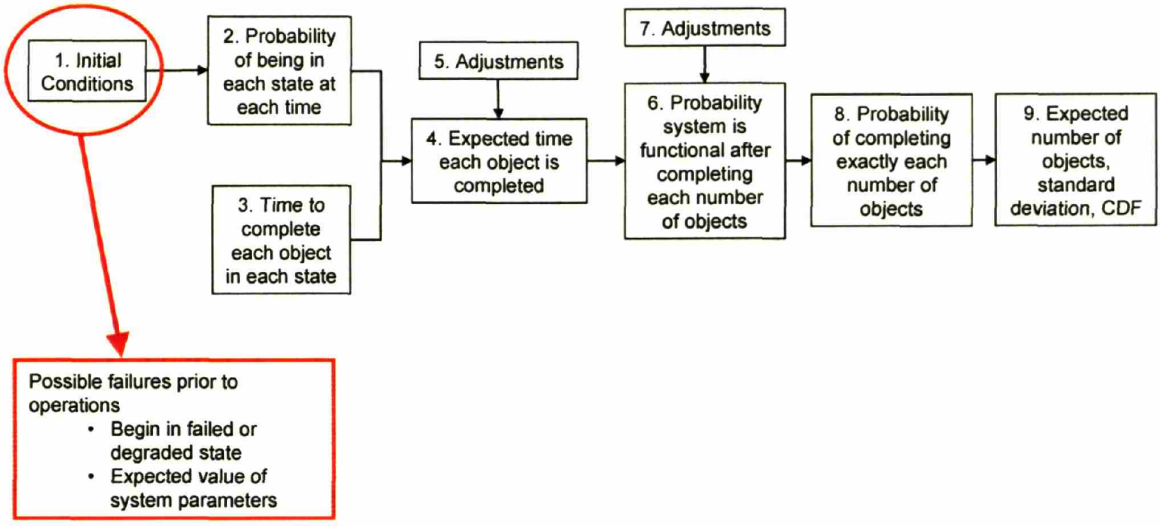


Figure 3-2: Determining Initial Conditions from Possible Failures Prior to Operations

Many of the risk items identified for missions are single events that occur before operations. Examples of these include a launch failure or a deployment failure. These risks result in a change to the initial conditions used to find the probability of being in each state. The probability that the system is in a completely failed state before operations begin is the probability that at least one critical failure event occurred prior to operations. Care needs to be taken not to double count the probability of multiple critical failure events occurring, as shown by the overlap of events A and B in Figure 3-3.

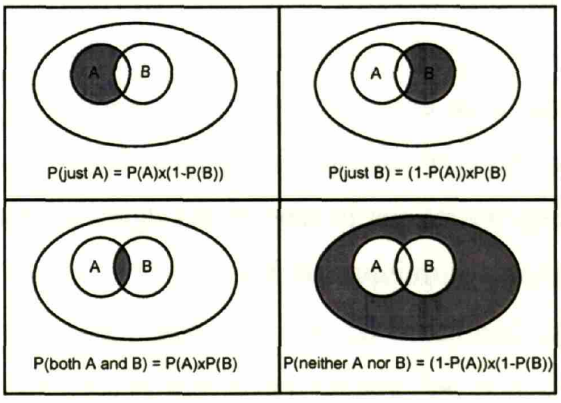


Figure 3-3: Four possible outcomes and their probabilities from two independent, probabilistic events.

If both A and B are critical failure events that occur prior to operations, then the probability that the mission is in a functional state at the beginning of operations, and therefore that neither A nor B has occurred, is given by Equation 3-1.

$$\begin{aligned} P(\text{neither A nor B}) &= 1-[P(\text{A})+P(\text{B})-P(\text{A and B})] \\ P(\text{neither A nor B}) &= 1-[P(A)+P(B)-P(\text{A})\times P(B)] \\ P(\text{neither A nor B}) &= 1\text{-}P(A)\text{-}P(B)+P(A)\times P(B) \end{aligned} \qquad (3\text{-}1)$$

A Matlab function has been created to determine the probability that at least one of any n independent events will occur given the probability of each individual event. This function can now be used to find the probability that the system is in a failed state before operations have begun, or P_{o_Failed}. This same function can be used to find the probability that the system begins operations in any degraded state captured in the state information matrix (the state information matrix will be discussed in Section 3.2.2). An example of beginning operations in a degraded state could occur if a particular component is not mission critical, and could fail either due to an anomaly prior to operations or due to a malfunction during operations. In this case, a degraded state of the system will be defined as the state in which the component has failed, and this degraded state will have a non-zero initial probability based on the probability of the anomaly prior to operations occurring.

The initial conditions are represented as a row vector that is eventually used as the first row of the $\boldsymbol{P}$ matrix, which is discussed in detail in Section 3.2.2. The entries in the row vector are the probabilities of being in each corresponding state at the beginning of operations. All of these initial probabilities, except the probability of beginning operations in the nominal state are calculated as discussed above. The probability of beginning operations in the nominal state is calculated as one minus the sum of the probabilities of beginning operations in any of the degraded states or the completely failed state. This logic is shown in Equation 3-2:

$$P_o(1) = 1 - \left(\left(\sum_{n=2}^{\#\text{ of states}} P_o(n) \right) + P_{o\_Failed} \right) \qquad (3\text{-}2)$$

where $P_o(n)$ is the probability of beginning operations in state n, and P_{o_Failed} is the probability of complete system failure prior to operations.

In addition to risk elements that decrease the probability of beginning operations in the nominal state, other risk elements increase the probability that the system will begin operations with degraded performance. Examples of these types of risk elements include a subsystem or technology not being developed to the required performance level or a partial deployment failure with which the system could still function, but at a reduced throughput rate or for a reduced time. These failure modes occur at or before the beginning of operations. Therefore, the initial system performance metrics, such as failure rates, lifetime, or efficiency, need to be adjusted before being used in conjunction with a dynamic failure model to find the overall expected total productivity. Using an observatory system example, a nominal system may have an observational efficiency of 1 (defined as equal time observing and non-observing). However, if control algorithms are not developed to the required level, the observational efficiency may be reduced to 0.5 (twice the time taking observations is spent on overhead). These algorithms will not mature to the required level with some probability, *Pc*. As an example, let us take the probability of these algorithms not being developed to be 0.1. As shown in Equation 3-3, the initial starting condition of this system is an expected observational efficiency value of 0.95.

$$\begin{aligned} E[\text{Initial Observational Efficiency}] &= 0.5 \times Pc + 1 \times (1 - Pc) = 0.05 + 0.9 \\ E[\text{Initial Observational Efficiency}] &= 0.95 \end{aligned} \qquad (3\text{-}3)$$

Once in operations, a single actuator may then fail. If this occurs, we assume for this example that the observational efficiency is once again cut in half. The productivity in the state in which a single actuator has failed should be based on an initial observational efficiency of 0.95, as shown in Equation 3-4.

$$\text{Obervational Efficiency in Degraded State} = \frac{1}{2} \times E[\text{Initial Observational Efficiency}]$$
$$\text{Obervational Efficiency in Degraded State} = \frac{1}{2} \times 0.95 = 0.475 \quad (3\text{-}4)$$

The example shown in Equations 3 and 4 is very simple. However, this shows only a single failure mode's effect on a system performance metric. In reality, many different failure modes will affect the expected value of the initial performance metrics. Therefore, it is important to develop a method to find the combined expected value of each of these metrics, given several independent events that could affect them. For example, assume there are two events that would decrease the initial observational efficiency. These events are totally independent; however, both have similar outcomes. Assume that both of these events would reduce the observational efficiency by a factor of two. There is now a chance, if both events occur, that the initial observational efficiency could be reduced by a factor of four compared to the original value. A method is needed to determine the expected value of a metric given several different probabilistic events that affect the value of that metric.

In general, the expected value is found by multiplying the probability of an event by the outcome of that event. In the case of two independent probabilistic events, there are four separate and unique outcomes. These outcomes were shown previously in Figure 3-3 and are defined as one or the other event occurring, both occurring, and neither occurring. Since the events are independent, the probability of each outcome can be calculated using the probability of either event individually occurring. For event A only to occur, event A needs to occur and event B cannot occur, and vice versa for event B only. If the probability of event A occurring is *Pa*, the probability of event A not occurring is *1-Pa*. Therefore, the probability of each outcome occurring is simply a combination of the probability of each event and/or one minus the probability of each event. All possible outcomes can be found easily by determining a full-factorial matrix for the number of events with two possible values each – 0 if the event did not occur and 1 if the event did occur. Then a probability vector can be found by starting with a probability of 1 for each case and multiplying by *Pa* if there is a 1 in the A column and

(1-Pa) if there is a 0 in the A column, and so on for other events. This is shown in Equation 3-5 for an example problem:

$$\vec{P} = \left[Pa \times (1 - Pb) \quad Pb \times (1 - Pa) \quad Pb \times Pa \quad 1 - (Pa + Pb - Pb \times Pa)\right] \tag{3-5}$$

Next, a value vector can be determined by starting with the initial condition and multiplying by the effect of event A if there is a 1 in the A column, and so on as with the probability vector. This is shown in Equation 3-6, assuming that either event would independently reduce the performance metric by a factor of 2:

$$\vec{V} = \begin{bmatrix} 0.5S \\ 0.5S \\ 0.25S \\ S \end{bmatrix} \tag{3-6}$$

where S is the initial system performance metric (such as observational efficiency). Finally, the dot product of the value vector and the probability vector can be used to get the total final expected value, as shown in Equation 3-7 for the example problem:

$$\begin{aligned} \vec{P} \cdot \vec{V} &= 0.5S \times Pa \times (1 - Pb) + 0.5S \times Pb \times (1 - Pa) + 0.25S \times Pb \times Pa + S \times (1 - (Pa + Pb - Pb \times Pa)) \\ \vec{P} \cdot \vec{V} &= S \times (0.5Pa - 0.5PbPa + 0.5Pb - 0.5PbPa + 0.25PbPa + 1 - Pa - Pb + PbPa) \\ \vec{P} \cdot \vec{V} &= S \times (1 - 0.5Pb - 0.5Pa + 0.25PbPa) = S \times (1 - 0.5Pb) \times (1 - 0.5Pa) \end{aligned} \tag{3-7}$$

Currently, we have assumed that the effects of individual events are multiplied together if two or more events occur; however, several other methods could be used, such as summing the effects together, or multiplying the effects for a few events and then assuming that after a given number of partial failures the whole system is considered completely failed. These other methods could be easily implemented using the approach described above, by simply adjusting the $\vec{V}$ vector.

3.2.2 Step 2: Determining the Probability of Being in Each State at Each Time

Once the initial conditions are set, the next step in determining the expected productivity of a path-dependent system is to find the probability of being in each degraded state throughout time. This is accomplished by using Markov modeling and the state-transition matrix. As discussed previously, a Markov modeling approach can be

used, even if the productivity is path-dependant, if the functional state of the system itself still depends only on the previous functional state. This step is shown and summarized in Figure 3-4, and discussed in detail below.

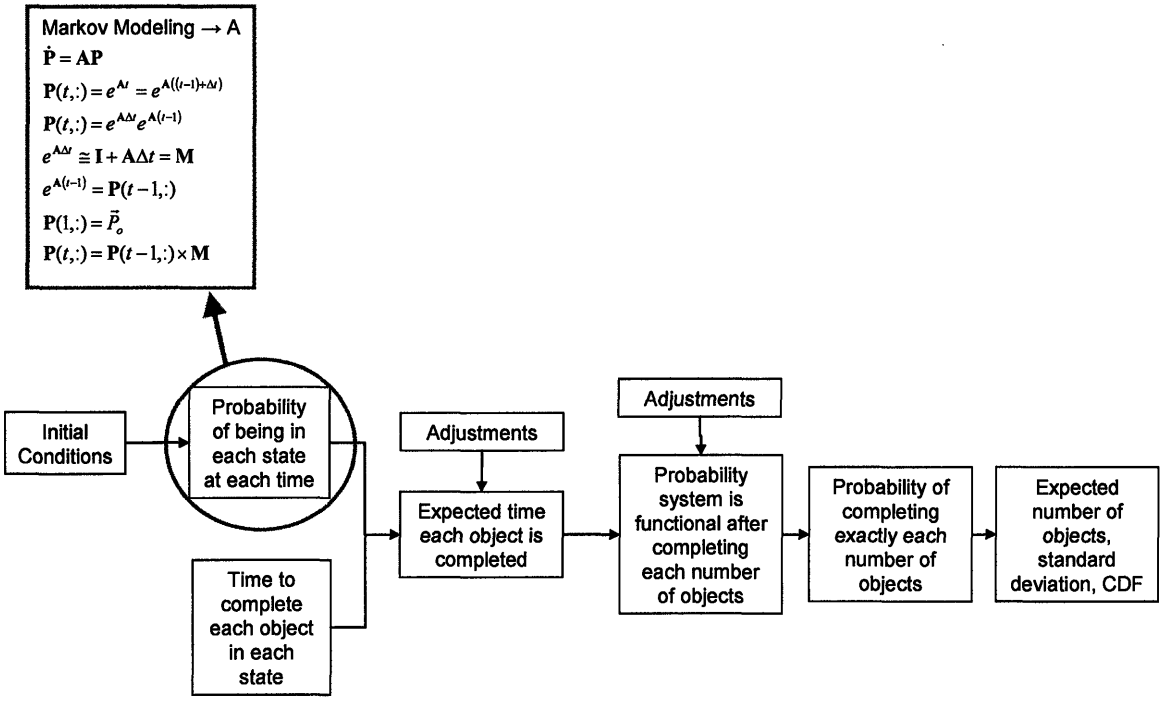


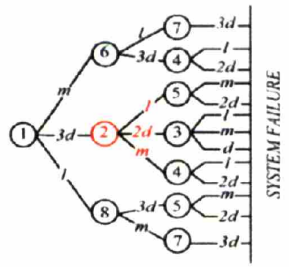
Figure 3-4: Probability of Being in Each State at Each Time

The state-transition matrix, also called the A matrix, defines both the states of a system and the rate at which the system will transition from one state to the next. The state of the system changes as failures occur in the system. The A matrix is found by analyzing the Markov model of a system. If $\vec{P}(t)$ is defined as the vector of probabilities of being in each state of the system at a particular time, the A matrix is defined as:

$$\frac{d\vec{P}(t)}{dt} = \mathbf{A}\vec{P}(t) \qquad (3\text{-}8)$$

The state-transition matrix is essential in calculating the probability of being in each state of the system, and therefore is also needed to calculate several important parameters of the entire system, such as productivity and reliability.

An A matrix can be created by looking at each state individually. Each row and column of the matrix corresponds to a different state. Figure 3-5 shows a very simple example of a state diagram, or Markov model, and the corresponding A matrix.



A=

-3d-m-l	0	0	0	0	0	0	0
3d	-2d-m-l	0	0	0	0	0	0
0	2d	-d-m-l	0	0	0	0	0
0	m	0	-2d-l	0	3d	0	0
0	l	0	0	-2d-m	0	0	3d
m	0	0	0	0	-3d-l	0	0
0	0	0	0	0	l	-3d	m
l	0	0	0	0	0	0	-3d-m

Figure 3-5: Markov model and corresponding A matrix for a sample system of three dual functioning spacecraft, one combining spacecraft, and one collecting spacecraft.

In Figure 3-5 d, m, and l are the failure rates of three different components – component "D", component "M", and component "L". The diagonal entries of the A matrix correspond to the ways in which the system could leave that state. In the example shown in Figure 3-5, three independent components could fail in state two. As a result, the diagonal entry for the second row would be minus one times the sum of the failure rates of each of the three components, as shown in Equation 3-9:

$$\mathbf{A}(2,2) = -(2d + m + l) \qquad (3\text{-}9)$$

If a component fails in a given state and the system is still operating but in a different state, then the column entry of the new state's row would contain the rate at which this process occurs. Consider the example shown in Figure 3-5, where when a component fails the system transitions from the second to the third, fourth, or fifth state. In the A matrix representation, the third, fourth, or fifth row and second column entry would be the failure rate of the failed component. The system transitions from the second to the fifth state if a "L" component fails. Therefore, the fifth row and second column entry of

the A matrix is the failure rate of the collecting spacecraft, or l, as shown in Equation 3-10:

$$\begin{aligned} \mathbf{A}(5,2) &= l \\ \mathbf{A}(4,2) &= m \end{aligned} \qquad (3\text{-}10)$$

Since there are two identical "D" components in the system in state two, and if either one of them fails the system is considered in the third state, the corresponding third row and second column entry of the A matrix would be two times the failure rate of the component, as shown in Equation 3-11:

$$\mathbf{A}(3,2) = 2d \qquad (3\text{-}11)$$

Any entry of the matrix that is not on the diagonal and does not connect one state to another is simply zero.

To generate the A matrix in an efficient manner for many different systems, a recursive, automatic A matrix generation Matlab function has been developed [Wertz, 2002]. Once the pattern to the A matrix has been identified and understood, the main challenges in automating the process of creating the A matrix are defining the states, checking if a new state has been previously defined or not, knowing when a failure causes the system to move to a new state, and identifying when the entire system has failed.

Both the state-transition matrix itself and a matrix containing the state information are simultaneously inputs and outputs to the recursive function used to automatically generate the A matrix. Each row of the state information matrix corresponds to a particular state and completely identifies that state. Examples of columns in the state information matrix include the number of functioning components of a particular type (e.g. 2 transmitters) or a binary variable to identify if a particular aspect of the system is functioning or not (e.g. 1 if the antenna is functional, 0 if the antenna has failed). Each one-by-n row vector from the state information matrix is unique for that given state, such that by checking if the one-by-n vector identifying a particular state is already a row of the state information matrix, it is possible to see if that given state has previously been defined. If this vector is not already a row of the state information matrix, the state should

be added as a new state. An additional variable is passed as another input to the function to identify the row number of the previous state, from which the current state was derived. This allows the entries for all states to be entered in both the correct rows and columns of the A matrix. A flow diagram showing this process is shown in Figure 3-6.

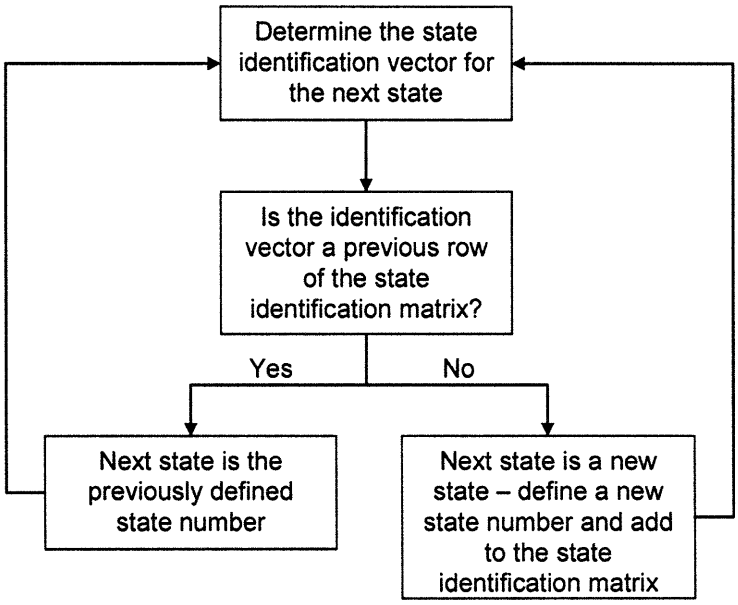


Figure 3-6: Flow chart showing the state information matrix definition process.

The automatic A matrix generation code is a recursive function, meaning that it calls itself within the function. The function has built in rules that decide whether a given state definition is acceptable and could be a new state, or if the system has failed. Consider the example of a formation flight interferometer system with three different types of spacecraft - collecting spacecraft, combing spacecraft, and dual functioning spacecraft which can collect or combine light but not do both at the same time. Assume that the system requires two spacecraft capable of collecting light and one capable of combining light to be functional. The operational rules for such a system are:

1. The number of spacecraft acting as collecting spacecraft must be greater than or equal to two. This includes both the collecting spacecraft and the dual functioning spacecraft.

2. The number of spacecraft acting as combining spacecraft must be greater than or equal to one. This includes both the combining spacecraft and the dual functioning spacecraft.

3. Since the dual functioning spacecraft cannot collect and combine light at the same time, and since both two collecting spacecraft and one combining spacecraft must be working for the system to be operational, the total number of spacecraft must be greater than or equal to three.

Since the A and state information matrices are both inputs and outputs in each call to the automatic A matrix generation function, they are continuously updated. If altering the status of any one column in the state information matrix leads to a state that satisfies the operational rules, the function is called again with the new state identifier. If altering the status of any one column in the state information matrix causes the system to fail the operational rules tests, the current state must lead directly to system failure if that component fails and the function is not called again.

One call to the recursive automatic A matrix generation function will automatically produce the full A matrix and the full state information matrix. The state information matrix can then be used to calculate the productivity in each state while the A matrix is used to calculate the probability of being in each state throughout time. More information on the details of the recursive automatic A matrix generation function are available in [Wertz, 2002].

The probability of being in any given state at any given time is calculated using numerical integrations of Markov models [Babcock, 1986]. The method involves transforming the A matrix from a continuous time matrix to a discrete time matrix, M, as shown in Equation 3-12, where Δt is the duration of the time step and $\mathbf{I}$ is the identity matrix.

$$\mathbf{M} = \mathbf{I} + \mathbf{A}\Delta t \qquad (3\text{-}12)$$

Define ***P*** as a matrix of the probabilities of being in each state at each time. The vector of the probabilities of being in each state at a given time, ***P(t,:)***, can be found by integrating the definition of the ***A*** matrix, given in Equation 3-8. This is shown is Equation 3-13:

$$\begin{aligned} \dot{\mathbf{P}} &= \mathbf{AP} \\ \mathbf{P}(t,:) &= e^{\mathbf{A}t} \end{aligned} \qquad (3\text{-}13)$$

We can break t into the time at the end of the previous time step plus the length of the time step.

$$\mathbf{P}(t,:) = e^{\mathbf{A}t} = e^{\mathbf{A}((t-1)+\Delta t)} \qquad (3\text{-}14)$$

Simplifying, we get:

$$\mathbf{P}(t,:) = e^{\mathbf{A}\Delta t} e^{\mathbf{A}(t-1)} \qquad (3\text{-}15)$$

Remembering the Taylor series expansion, the first term in Equation 3-15 is an approximation for the ***M*** matrix.

$$e^{\mathbf{A}\Delta t} \cong \mathbf{I} + \mathbf{A}\Delta t = \mathbf{M} \qquad (3\text{-}16)$$

From Equation 3-12, the second term in Equation 3-15 is the previous row of the ***P*** matrix.

$$e^{\mathbf{A}(t-1)} = \mathbf{P}(t-1,:) \qquad (3\text{-}17)$$

We already know that the first row of the ***P*** matrix is the initial conditions that were calculated in Section 3.2.1.

$$\mathbf{P}(1,:) = \vec{P}_o \qquad (3\text{-}18)$$

Substituting Equation 3-16 and Equation 3-17 into Equation 3-15, we can find the rest of the rows of the ***P*** matrix by multiplying the probability of being in each state from one time step before by the ***M*** matrix, as shown in Equation 3-19:

$$\mathbf{P}(t,:) = \mathbf{P}(t-1,:) \times \mathbf{M} \qquad (3\text{-}19)$$

Note that the rows of ***P*** correspond to time steps, and the columns correspond to states. Therefore, to know the probability of being in state two (as defined by the second row of the state information matrix), during time step five, one would look at ***P***(5,2).

3.2.3 Step 3: Time to Complete Each Object in Each State

The time to complete each object in each state is calculated using a productivity model. This step in the overall flow is shown in Figure 3-7. As a reminder, throughout this discussion, an object is defined as a single unit of the performance metric. Examples of an object include a measurement or an image. The time to complete a particular object is calculated using a productivity model. This time will depend on both the characteristics of that object and the functional state of the system. In degraded states, the productivity of the system is generally lower, resulting in a longer time to complete a given object. Additionally, in some degraded states it will not be physically possible to complete certain objects. Whether or not an object can be completed in a particular degraded state will also be determined by the productivity model.

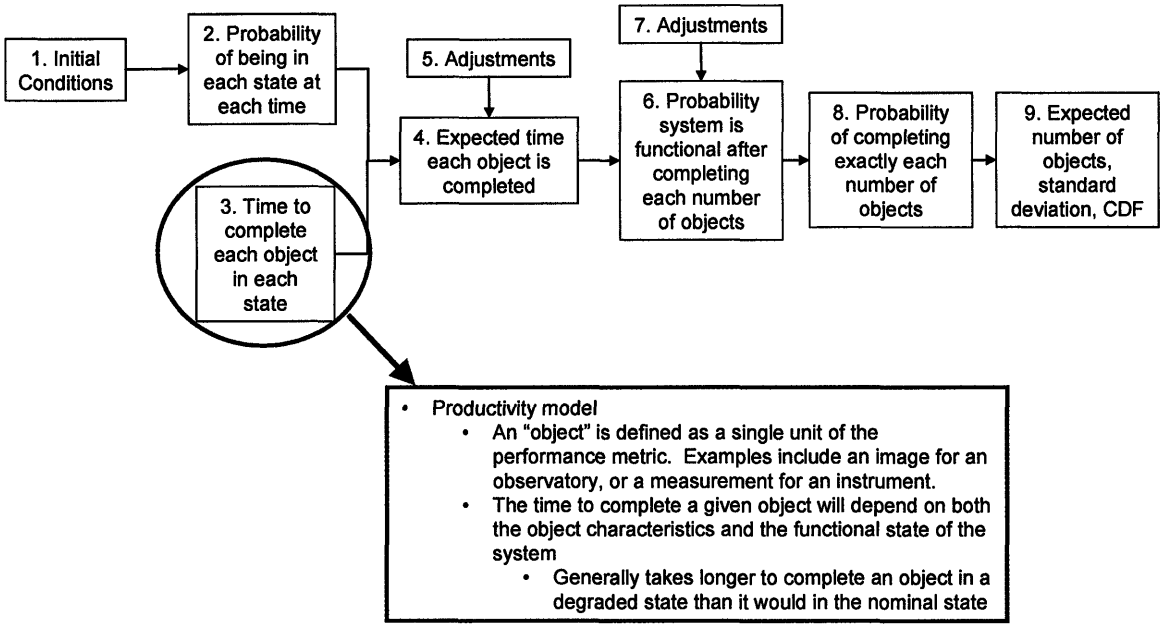


Figure 3-7: Time to complete each object in each state

The first step in the "time to complete each object" calculation is to decide the order in which objects will be completed. Adjustments to this order will be made in future steps to account for various situations, but an initial ordering must be set for the simulation. In some cases, the order of objects may be set based on a given preference of

the stake-holders. If a pre-determined order is not set based on preferences, then the objects are sorted in terms of increasing time required in the nominal state. This is logical because the most likely scenario is that a failure will not occur, leaving the system in the nominal state, and therefore the objects will be completed in the optimal order of shortest to longest completion times.

The time required to complete an object can be transformed into the number of time steps required to complete the object. This is shown in Equation 3-20:

$$\vec{T} = \frac{\vec{t}}{\Delta t} \qquad (3\text{-}20)$$

where $\vec{t}$ is a vector of the times required to finish the object in each state, Δt is the length of a time step, and $\vec{T}$ is a vector of the number of time steps required to finish the object in each state. If it is not possible to complete the object in a given state, the time required in that state is reported as zero.

In situations where it is possible to complete an object in a degraded state, but not in the nominal state, a minor adjustment must be made to the $\vec{t}$ vector, or the vector of the required times to complete the object in each state. While this situation is extremely rare, it does occur, usually when the degraded state can complete different, but not more, objects than the nominal state. It is assumed that if an object can be completed in a degraded state, the system would be able to change to this state from the nominal state to complete the object. Therefore, in this situation, the time required to complete the object in the degraded state is used as the required time in both the nominal *and* degraded states.

3.2.4 Step 4: Expected Time to Complete Each Object

The next step is to find the expected number of time steps to complete each object. This step is shown in Figure 3-8 and discussed in more detail below.

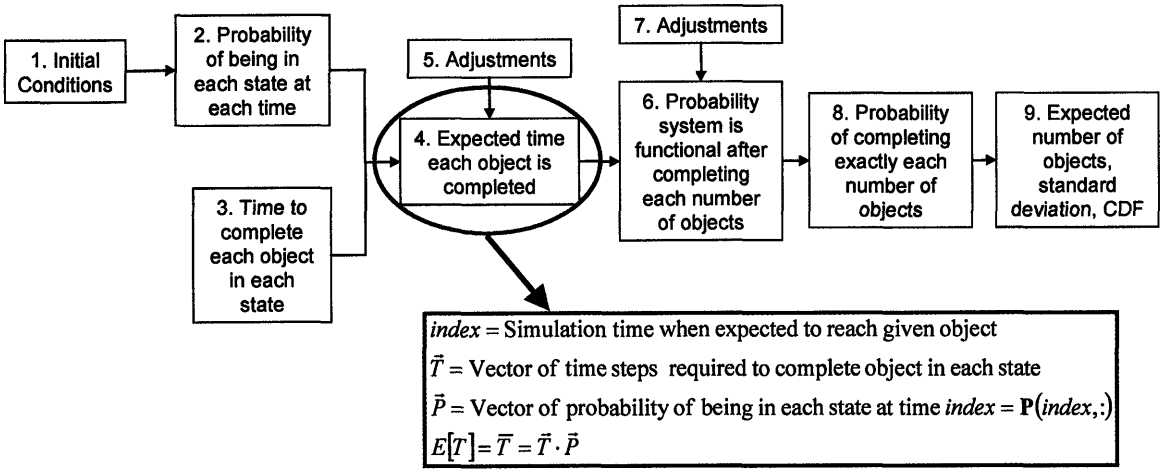


Figure 3-8: Expected time to complete each object

First, we need to find the index of the number of time steps corresponding to the simulation time when a particular object is begun. This is shown in Equation 3-21:

$$index = \frac{time}{\Delta t} \qquad (3\text{-}21)$$

where *time* is the current simulation time and Δt is the length of a time step.

The probability of being in each state at the beginning of the object can be found by looking up the row *index* in the probability matrix, **P**. The number of time steps required to complete the object in each state is calculated using the productivity model, as discussed in Section 3.2.3. The expected number of time steps required to complete the object is then calculated by multiplying the number of time steps required in each state by the probability of being in that state at the beginning of the object. This is shown in Equation 3-22:

$$E[T] = \overline{T} = \vec{T} \cdot \vec{P}^T \qquad (3\text{-}22)$$

where, $\overline{T}$ is the expected number of time steps, $\vec{T}$ is the vector of time steps required to complete the object in each state, and $\vec{P}$ is the vector of the probability of being in each state at time *index*, or **P**(*index*, :).

3.2.5 Step 5: Adjustments to the Expected Time to Complete Each Object Calculation

A few adjustments to the calculations that determine the expected time to complete each object are required to account for specific situations and details. These adjustments are summarized in Figure 3-9, and discussed in detail below.

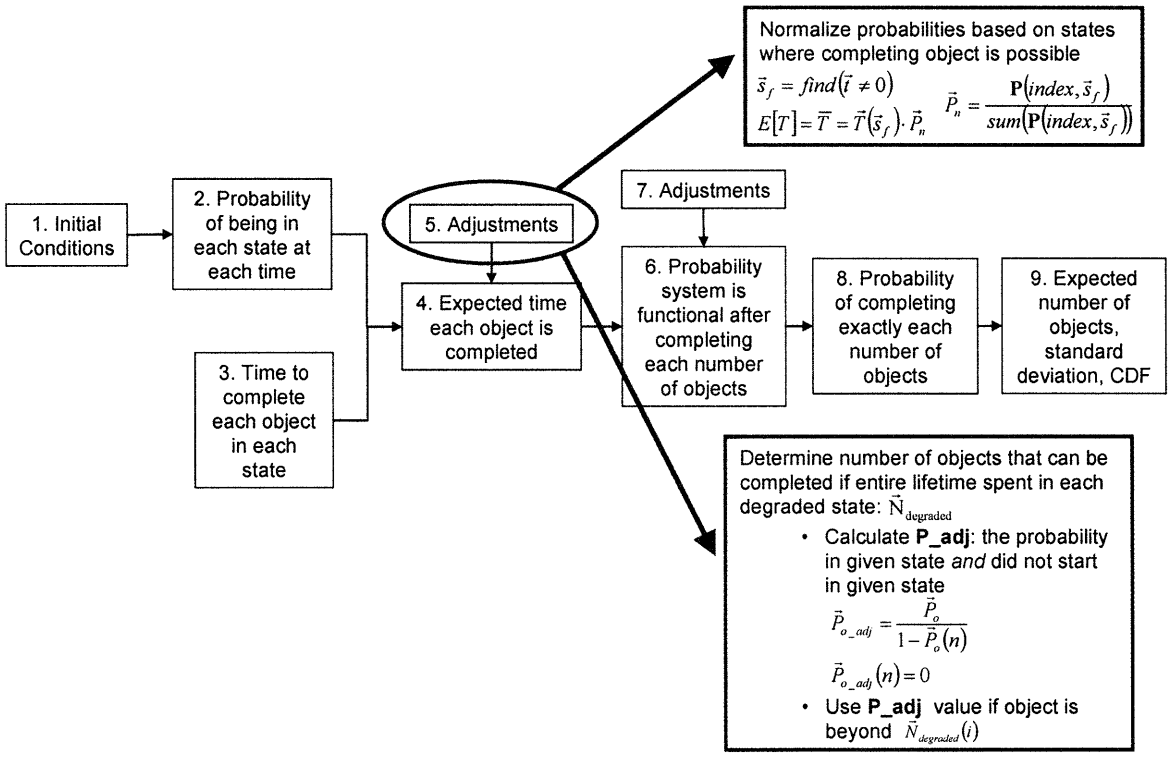


Figure 3-9: Adjustments to the expected time to complete each object calculation

When finding the expected number of time steps to complete an object, it is important to first normalize the probabilities that the system is in each state based on only those states in which completing the object is possible. Therefore, the calculated value for the expected time to complete an object is actually the expected time to complete the object given that the object can be completed. First, the states in which it is possible to complete the object are identified, as shown in Equation 3-23:

$$\vec{W} = find(\vec{T} \neq 0) \qquad (3\text{-}23)$$

where the *find* function returns the index of the vector entries that match the given criteria, and $\vec{W}$ is a vector of all states in which the system can complete the given object, called the "working vector." Next, the normalized probabilities can be calculated, as shown in Equation 3-24:

$$\vec{P}_{norm} = \frac{\mathbf{P}\left(index, \vec{W}\right)}{sum\left(\mathbf{P}\left(index, \vec{W}\right)\right)} \qquad (3\text{-}24)$$

where $\vec{P}_{norm}$ is the vector of normalized probabilities, $\mathbf{P}$ is the probability matrix, and *index* is the current time step in the simulation. Finally, the expected number of time steps to complete the object is calculated using the normalized probabilities, as shown in Equation 3-25:

$$E[T] = \overline{T} = \vec{T}\left(\vec{W}\right) \cdot \vec{P}_{norm} \qquad (3\text{-}25)$$

Perhaps the best method to describe this adjustment is to look at a simple example. Suppose we have a system with three states – nominal, partially failed, and completely failed. In addition, suppose that at the current time in the simulation, we have an equal chance of being in any of the three states, as shown in Equation 3-26:

$$\mathbf{P}(index,:) = \begin{bmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{bmatrix} \qquad (3\text{-}26)$$

In the nominal state, it takes two time steps to complete the current object. In the partially failed state, this same object requires four time steps, and in the completely failed state, the object cannot be completed. These time step requirements are shown in Equation 3-27:

$$\vec{T} = \begin{bmatrix} 2 & 4 & 0 \end{bmatrix} \qquad (3\text{-}27)$$

To find the expected number of time steps required to complete our object, we must first find the states in which completing an object is possible:

$$\vec{W} = \begin{bmatrix} 1 & 2 \end{bmatrix} \qquad (3\text{-}28)$$

Next, we must renormalize the probabilities of being in the two working states, shown in Equation 3-29.

$$\vec{P}_{norm} = \frac{\left\lfloor \frac{1}{3} \quad \frac{1}{3} \right\rfloor}{\frac{1}{3}+\frac{1}{3}}$$

$$\vec{P}_{norm}(1) = \frac{\frac{1}{3}}{\frac{1}{3}+\frac{1}{3}} = \frac{1}{2} \qquad (3\text{-}29)$$

$$\vec{P}_{norm}(2) = \frac{\frac{1}{3}}{\frac{1}{3}+\frac{1}{3}} = \frac{1}{2}$$

Finally, we find the total expected number of time steps required, given that the object can be completed, shown in Equation 3-30:

$$E[T] = \bar{T} = [2 \quad 4] \cdot \left\lfloor \frac{1}{2} \quad \frac{1}{2} \right\rfloor$$
$$\bar{T} = \frac{1}{2} \times 2 + \frac{1}{2} \times 4 = 3 \qquad (3\text{-}30)$$

In certain cases, an adjustment must also be made to the ***P*** matrix to account for situations in which mission lifetime will run out in degraded states before the number of objects the system is capable of completing in those states runs out. Take, for example, a case where completing an object in the degraded state takes twice as long as completing that same object in the nominal case. If in the nominal case this system can complete *x* objects, then if the system started life in the degraded state it could only complete approximately *x/2* objects (this number may vary based on the spread of times to compete each object, but for this example it can be approximated as *x/2*). The first reaction may be to correct for this problem by setting the time required to complete each object after object *x/2*, or whatever the limit to the degraded state system is, to zero. This would be equivalent to stating that all objects after this object could not be completed in the degraded state, even if the system has the capability to complete them, because time has run out. While this statement is accurate if the system began life in the degraded state, it

is not accurate if the system transferred to the degraded state through a failure at some point during the lifetime of the mission. Accounting for the exact scenario of the system transitioning to the degraded state at every possible time step would be too complex and would make the computation effort and time required too much to be useful in a trade tool. Additionally, transferring to the degraded state at some point throughout life is already covered by using the *expected* time to complete objects to calculate the overall productivity. Therefore, an adjustment is made to account only for the situation in which the system transferred to the degraded state prior to operations.

To account for the situation discussed above, the probability matrix, ***P***, is adjusted for all objects after the final object that the system could complete if it was in the degraded state for the entire lifetime. In actuality, the probability of completing these objects is not zero, but is a reduced value. In other words, there is still some probability that the system transitioned to the degraded state sometime during operations, as opposed to prior to operations, therefore allowing for the possibility that the object in question could still be completed within the allotted time. Therefore, it is necessary to reduce the value in the probability matrix for these objects from the probability of being in the degraded state, to the probability of being in the degraded state at this time *and* not being in the degraded state at the beginning of life.

The first step to this adjustment is to determine which objects to adjust, i.e. the objects that are beyond the limit of what can be completed if the entire lifetime is spent in the degraded state. The time required to complete each object in each degraded state is already calculated to find the expected time required for each object. The number of objects that can be completed in a particular state throughout the entire lifetime can be calculated by summing up the previously calculated required times to complete each object. This number of objects will be called $\vec{N}_{degraded}$, with each entry of the vector corresponding to a particular state.

Next, an adjusted ***P*** matrix can be calculated, called ***P_adj***. The values in this matrix correspond to those in the ***P*** matrix; however, the adjusted values are the probabilities that the system is in each state *given* that the system did not begin operations in that state. Each column of this matrix is calculated in exactly the same fashion as the ***P*** matrix, but with the initial conditions set to zero for the given state and the probability

of being in each other state normalized to account for zero probability in the given state. The process of calculating ***P_adj*** is shown in Equation 3-31:

$$\begin{aligned}
&\vec{P}_{o_adj} = \frac{\vec{P}_o}{1-\vec{P}_o(n)} \\
&\vec{P}_{o_adj}(n) = 0 \\
&\mathbf{P_adj}_n(1,:) = \vec{P}_{o_adj} \\
&\mathbf{P_adj}_n(t,:) = \mathbf{P_adj}_n(t-1,:)\mathbf{M} \\
&\mathbf{P_adj}(:,n) = \mathbf{P_adj}_n(:,n)
\end{aligned} \tag{3-31}$$

where n varies from two through the total number of states. Note that the columns of ***P_adj*** corresponding to the first state, in addition to any state in which $P_o(n)$ is zero, will be equal to the original ***P*** matrix and do not need to be recalculated. The ***P_adj*** matrix will be used later in the process to find the probability that the system is not only in the degraded state, but also has not been in that degraded state for the entire lifetime.

For all objects after $\vec{N}_{degraded}(n)$, the probability of being in the degraded state n, is adjusted to account for the probability that the entire lifetime of the mission has been spent in that state. The probability in the ***P*** matrix is the probability that the system is in a particular degraded state at a particular time. This probability needs to be adjusted to become the probability that the system is in a particular degraded state at this time, and it also did not begin operations in this state. We now have two known, calculated, values – ***P_adj***, the probability that the system is in this state at this time given that it did not start in this state, and $\left(1-\vec{P}_o(n)\right)$, the probability that the system did not start in this state. We are looking for the probability that both of these events occurred. From probabilistic theory, we know that:

$$P(AB) = P(A)P(B \mid A) \tag{3-32}$$

If we now substitute the event that the system did not begin in this state for event A by setting $P(A)$ equal to $\left(1-\vec{P}_o(n)\right)$, and substituting the event that the system is in the degraded state at this time for event B, setting $P(B|A)$ equal to ***P_adj***, we have everything we need to calculate the probability that the system both started in the nominal state and is now in the degraded state, $P(AB)$. Therefore, the values of the entries in the ***P*** matrix

are substituted for $\left(1-\vec{P}_o(n)\right)$ times the appropriate entry of the ***P_adj*** matrix for all time steps beyond the expected time to begin the next object after $\vec{N}_{degraded}(n)$. This process is shown in Equation 3-33:

$$P_{New}=\begin{bmatrix} P(1,1) & P(1,2) & \cdots & P(1,n) \\ P(2,1) & P(2,2) & \cdots & P(2,n) \\ \vdots & \vdots & \vdots & \vdots \\ P(a,1) & \left(1-\vec{P}_o(2)\right)\times P\_adj(a,2) & \cdots & P(a,n) \\ P(a+1,1) & \left(1-\vec{P}_o(2)\right)\times P\_adj(a+1,2) & \cdots & P(a+1,n) \\ \vdots & \vdots & \vdots & \vdots \\ P(b,1) & \left(1-\vec{P}_o(2)\right)\times P\_adj(b,2) & \cdots & \left(1-\vec{P}_o(n)\right)\times P\_adj(b,n) \\ P(b+1,1) & \left(1-\vec{P}_o(2)\right)\times P\_adj(b+1,2) & \cdots & \left(1-\vec{P}_o(n)\right)\times P\_adj(b+1,n) \\ \vdots & \vdots & \vdots & \vdots \end{bmatrix} \quad (3\text{-}33)$$

where a is the expected time step where object ($\vec{N}_{degraded}(2)+1$) is begun, and b is the expected time step where object ($\vec{N}_{degraded}(n)+1$) is begun.

3.2.6 Step 6: Probability that the System is Functional after Completing Each Number of Objects

Once the expected number of time steps to complete an object has been calculated, this information can then be used to find the probability that the system is function after completing each number of objects. This is shown in Figure 3-10 and discussed in detail below.

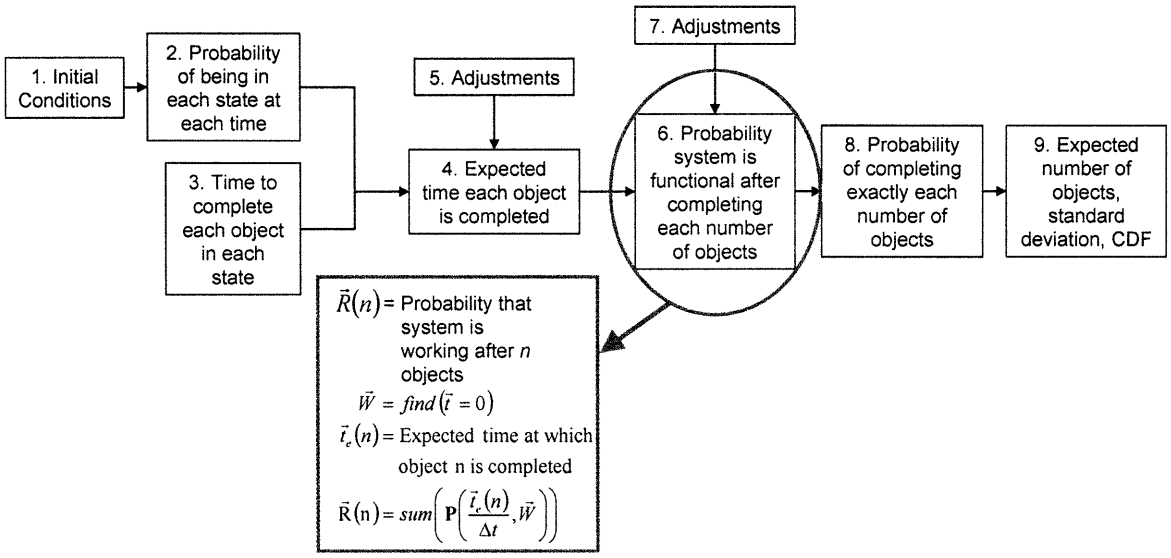


Figure 3-10: Probability that the system is functional after completing each number of objects

For each time step, the probability of being in each of the functioning and partially functioning states can be summed, resulting in the probability that the system is not in a completely failed state at that time. The vector of the identification numbers of the states in which the system is functional, or working, will be called the working vector, or $\vec{W}$. Clearly, if an object cannot be completed in a degraded state then that state is not considered a "working" state for that object. However, if the next object can be completed in this degraded state, then for that object the state is listed in the working vector. Therefore, $\vec{W}$ needs to be calculated on a per-object basis, and includes only those states that are not only defined as a functioning state, but are also capable of completing the given object. As mentioned previously, if it is not possible to complete an object in a given state, the productivity model will return a value of zero. Therefore, it is possible to identify the states that should be included in the working vector by identifying those states for which the productivity model has returned a non-zero value. This is shown in Equation 3-34:

$$\vec{W} = find(\vec{t} \neq 0) \qquad (3\text{-}34)$$

where $\vec{t}$ is the vector of times to complete the given object returned by the productivity model, and the *find* function returns the index of the vector entries that match the given criteria.

Using the expected time to complete each given object, the index of the time step at which it is expected that the system will be done completing that object can be calculated. Define $\vec{R}(n)$ as the probability that the system is in a working state at the end of the nth object, as shown in Equation 3-35:

$$\vec{\mathrm{R}}(\mathrm{n}) = sum\left(\mathbf{P}\left(\frac{\vec{t}_e(n)}{\Delta t}, \vec{W}\right)\right) \qquad (3\text{-}35)$$

where $\vec{t}_e(n)$ is the time at which object n is expected to be completed, Δt is the length of a time step, and **P** is the probability matrix (rows are time steps, columns are states).

3.2.7 Step 7: Adjustments to the Probability that the System is Functional after Completing Each Number of Objects Calculation

A few adjustments to the calculations that determine the probability that the system is functional after completing each number of objects are required to account for specific situations. These adjustments are summarized in Figure 3-11, and discussed in detail below.

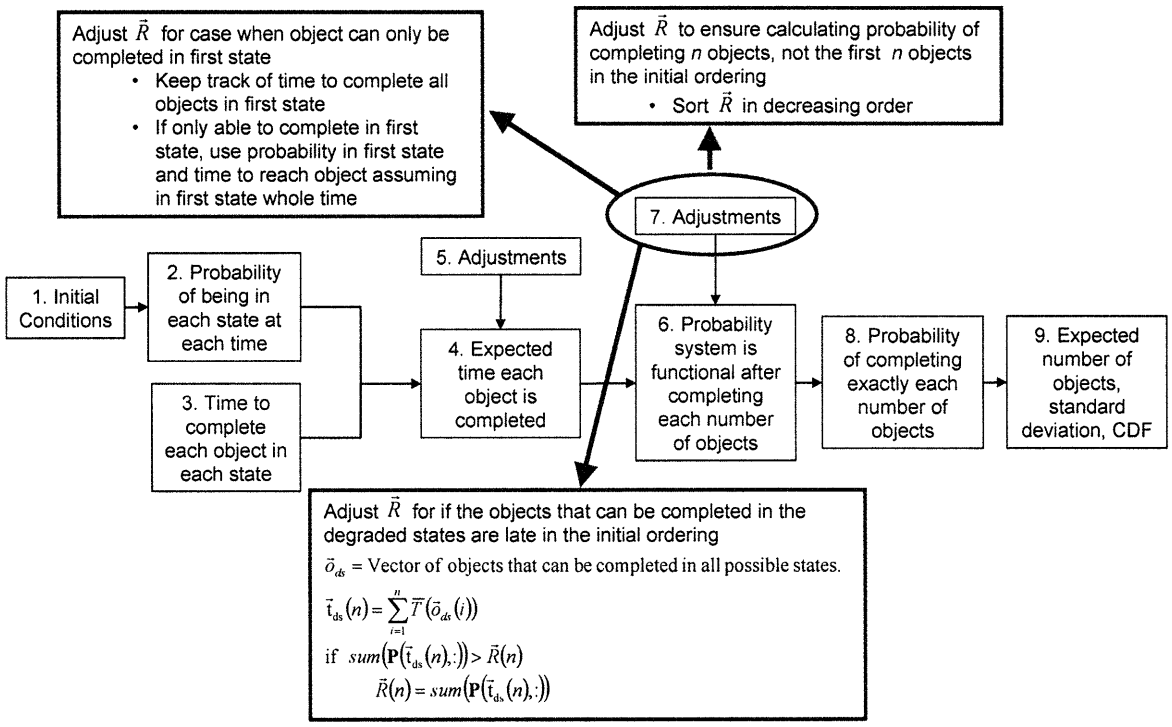
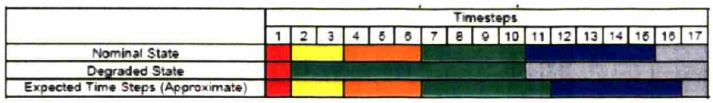


Figure 3-11: Adjustments to the calculation of the probability that the system is in a functional state at the end of each number of objects

The $\vec{R}$ vector is defined as the vector of probabilities that the system is in a working state at the end of each object. The first adjustment to the $\vec{R}$ vector accounts for situations when the system never leaves the first state. In this situation, it is possible to calculate the exact time needed to complete each object. The only cases where it is clear that the system never left the first state are cases where the last *n* objects in the initial ordering could only be completed in the first state. In these cases, either the system completed the objects still in the first state, or it did not complete the objects at all. Instead of using the expected time to complete each object, it is possible to use the time needed to complete all objects up to that point in the first state alone. To account for this possibility, the amount of time needed to complete each object in the first state needs to be recorded in addition to the expected time to complete each object. This first state time is then used to determine $\vec{R}(i)$ for any object in which that object, and any objects later in the list of objects, can only be completed in the first state.

The first adjustment to the $\vec{R}$ vector is illustrated in Figure 3-12 through a simple example. The time steps required to complete each object in each state are given at the top of the figure. Also provided are the probabilities of being in each state at each time, along with the expected number of time steps required to complete each object. With these probabilities and expected time steps, the original $\vec{R}$ vector can be calculated, and is shown in Figure 3-12a. The first adjustment, which was discussed above, is shown in Figure 3-12b, with the affected entry of the $\vec{R}$ vector highlighted in blue.

A second adjustment to the $\vec{R}$ vector is needed to account for situations in which the initial ordering of objects did not place all objects that can be completed in a degraded state first. $\vec{R}(n)$, as calculated previously, is the probability of being in a functioning or partially functioning state at the end of the expected time to complete object *n*, but is meant to represent the probability that the system will still be functional after completing *n* objects. There is nothing about $\vec{R}(n)$ that implies that the system needs to complete objects in the order that was used to estimate the time to complete each object. In other words, if the second object cannot be completed in a degraded state, but the third object can, then the probability of completing at least two objects will be the probability of being in the nominal state at the end of two objects *or* in the degraded state at the end of the *third* object. Therefore, when completing the calculations for $\vec{R}(n)$ it is important to remember that if $\vec{R}(n)$ is less than $\vec{R}(n+1)$, then objects *n+1* and *n* may be switched in order depending on the state of the system at that time. To account for this, $\vec{R}$ is sorted in increasing order. In this sense, $\vec{R}$ still holds the same meaning, but the order of the objects is simply switched to account for those objects that may be more likely to be completed, since they can be completed in the degraded states. The $\vec{R}$ vector should be viewed as a vector of values, $\vec{R}(n)$, that represent the probability of the system being in a functioning state after completing *any n* objects, and not the particular first *n* objects in the initial ordering. This second adjustment is also illustrated in Figure 3-12c, again with the affected entry of the $\vec{R}$ vector highlighted in blue.



	Timesteps, Nominal	Timesteps, Degraded
Object 1	1	1
Object 2	2	0
Object 3	3	0
Object 4	4	9
Object 5	5	0

Time-steps	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Probability in Nominal State	0.9	0.88	0.85	0.83	0.8	0.78	0.75	0.73	0.7	0.68	0.65	0.63	0.6	0.58	0.55	0.53	0.5
Probability in Degraded State	0.05	0.07	0.09	0.11	0.13	0.15	0.17	0.19	0.21	0.23	0.25	0.27	0.29	0.31	0.33	0.35	0.37

	Expected Number of Time Steps
Object 1	1
Object 2	2
Object 3	3
Object 4	5
Object 5	5

	R(i) - Original
Object 1	0.945
Object 2	0.825
Object 3	0.750
Object 4	0.895
Object 5	0.5

a. Original R(i)

	P(State 1 only)
1 Object	0.9
2 Objects	0.825
3 Objects	0.75
4 Objects	0.650
5 Objects	0.525

Nominal state only adjustment

	R(i) - w/ Adjustment 1
1 Object	0.945
2 Objects	0.825
3 Objects	0.75
4 Objects	0.895
5 Objects	0.525

b. Adjustment 1: Nominal state only

	R(i) - w/ Adjustment 1
1 Object	0.945
2 Objects	0.825
3 Objects	0.75
4 Objects	0.895
5 Objects	0.525

Degraded state possible for only some objects (sort)

	R(i) – Sorted, w/ Adjustment 1
1 Object	0.945
2 Objects	0.895
3 Objects	0.825
4 Objects	0.750
5 Objects	0.525

c. Adjustment 2: Sorting

Number of objects that can be completed in all states	2
Total E(timesteps) to complete all objects from above	6
P(Nom or Deg State @ end of Timestep 6)	0.920

Degraded state late in initial ordering adjustment

	R(i) - Final
1 Object	0.945
2 Objects	0.920
3 Objects	0.825
4 Objects	0.750
5 Objects	0.525

d. Adjustment 3: Degraded state late in initial ordering

Figure 3-12 : Example of adjustments to the $\vec{R}$ vector.

The third and final adjustment to the $\vec{R}$ vector again accounts for situations in which the initial ordering of objects, based on the time to complete the objects in the

nominal state, is not optimal as degradations occur. This adjustment specifically accounts for situations in which only a few objects can be completed in a degraded state, and those objects are not near the beginning of the initial ordering. The probability of completing these objects is lowered by the fact that the ordering of objects places them near the end of life in the simulation, leaving the probability of being in a completely failed state higher than if they were attempted earlier in the order. In these cases, an adjustment needs to be made to account for situations in which the system either starts or transitions early to a degraded state. If the system is in a degraded state early in the life of the mission, then the probability of completing all the objects that the degraded states are capable of completing is higher than may have been previously calculated, since those particular objects will now be completed earlier. To account for this scenario, the total expected time required to complete all possible objects that can be completed in all degraded states is calculated. If the probability of being in a functioning state by the end of the time calculated is higher than the $\vec{R}$ vector entry for that number of objects, then this probability is used in the $\vec{R}$ vector in place of the previously calculated value. Essentially, this adjustment accounts for the fact that the probability values used for the objects that can be completed in all degraded states need to be adjusted for any re-ordering that occurred during the previous adjustment sorting the $\vec{R}$ vector.

This third adjustment is the final adjustment illustrated in Figure 3-12d, again with the affected entry of the $\vec{R}$ vector highlighted in blue. The final $\vec{R}$ vector can be seen in Figure 3-12d, and can be compared to the original $\vec{R}$ vector, shown in Figure 3-12a, to see the effect of all of the adjustments discussed above.

3.2.8 Step 8: Probability of Completing Exactly Each Number of Objects

The next step in the EPRA approach is to calculate the probability of completing exactly each number of objects. This step is summarized in Figure 3-13 and discussed in more detail below.

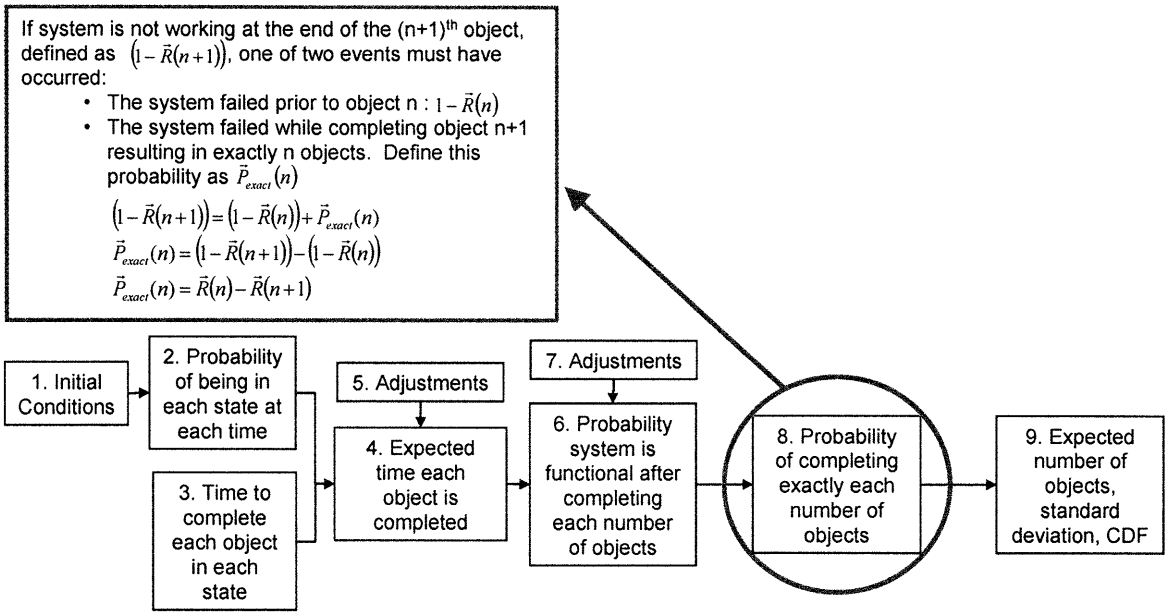


Figure 3-13: Probability of completing exactly each number of objects

For each object there are two possible outcomes: the object was completed or it was not completed. The probability that the object was completed is equal to the probability that the system is in a functioning or partially functioning state at the completion of the object, which is equal to $\vec{R}(n)$. Since the number of time steps required to complete the object is an expected value, which already takes into account the longer time needed to complete the object in partially failed states, it is assumed that if the system is in a functioning or partially functioning state at the required time, the object is completed. For the first object on the list there is a probability, equal to the probability that the system is in a completely failed state by the end of completing that first object, or $(1-\vec{R}(1))$, that no objects will be completed. There is also a probability, equal to the probability that the system is still in a functioning state at the end of the first object, but in a completely failed state by the end of the second object, that the system will complete exactly one object. Likewise, for the second object processed, there is a probability, equal to the probability that the system is functioning at the end of the second object but not at the end of the third object, that the instrument will complete exactly two objects. If

two events, A and B, are mutually exclusive, then the probability of either A or B occurring is the sum of the probabilities of either occurring. If event C is exhaustive in events A and B, and can therefore only occur if either event A or event B occurs, then P(C) = P(A) + P(B). In this case, if the system is not in a working state at the end of the *(n+1)th* object, which occurs with a probability of $\left(1-\vec{R}(n+1)\right)$, there are only two events which could have occurred. Either the system failed prior to finishing the n^{th} object, which occurs with a probability equal to $\left(1-\vec{R}(n)\right)$, or the system failed between the n^{th} and *(n+1)th* object, resulting in exactly *n* objects being completed, defined as $\vec{P}_{exact}(n)$.

$$\left(1-\vec{R}(n+1)\right)=\left(1-\vec{R}(n)\right)+\vec{P}_{exact}(n) \qquad (3\text{-}36)$$

Rearranging and simplifying Equation 3-36, it can be shown that the probability that the system completed exactly *n* objects, $\vec{P}_{exact}(n)$, is given by $\left(\vec{R}(n)-\vec{R}(n+1)\right)$. This is shown in Equation 3-37:

$$\begin{aligned}\vec{P}_{exact}(n)&=\left(1-\vec{R}(n+1)\right)-\left(1-\vec{R}(n)\right)\\ \vec{P}_{exact}(n)&=\vec{R}(n)-\vec{R}(n+1)\end{aligned} \qquad (3\text{-}37)$$

where $\vec{R}(n)$ is the probability of being in a functioning or partially functioning state at the mission elapsed time when object *n* is expected to be completed and $\vec{P}_{exact}(n)$ is the probability of completing exactly *n* objects.

3.2.9 Step 9: Expected Number of Objects, Standard Deviation, and CDF

The final step to the EPRA approach is to calculate the desired outputs: the expected number of objects (expected productivity); the standard deviation of this expected value; and the Cumulative Distribution Function (CDF). The output calculations are summarized in Figure 3-14, and discussed in more detail below.

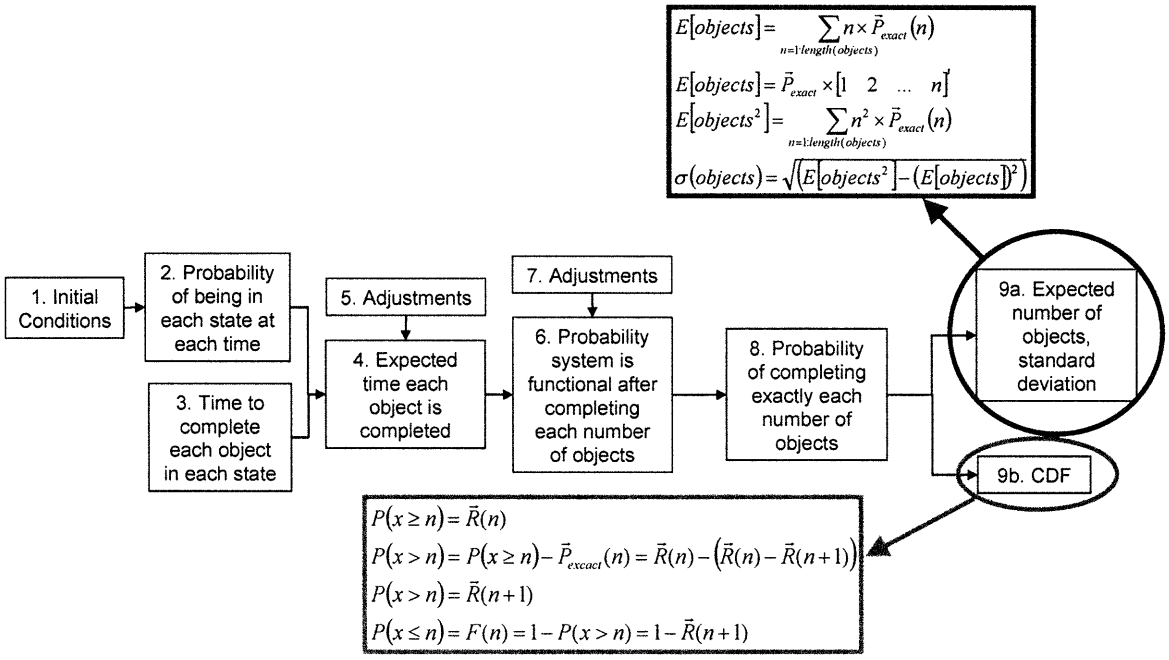


Figure 3-14: Calculating the EPRA outputs

Once the probability of completing exactly each number of objects is calculated, the expected number of objects completed is simply the probability times the number of objects, as shown in Equation 3-38.

$$E[objects] = \sum_{n=1:length(objects)} n * (\vec{R}(n) - \vec{R}(n+1)) \qquad (3\text{-}38)$$

Additionally, the expected number of objects squared, and therefore the standard deviation, can be calculated as shown in Equation 3-39.

$$E[objects^2] = \sum_{n=1:length(objects)} n^2 * (\vec{R}(n) - \vec{R}(n+1))$$
$$\sigma(objects) = \sqrt{(E[objects^2] - (E[objects])^2)} \qquad (3\text{-}39)$$

$\vec{R}(n)$ as calculated above is defined as the probability of being in a functioning or partially functioning state at the end of the expected time to complete object *n*. Therefore, the probability of completing at least *n* objects is equivalent to $\vec{R}(n)$. If a project has a goal of completing at least a given number of objects, the probability of

accomplishing that goal can now be calculated. Therefore, the architecture and failure rates required to meet that goal with a given probability can be calculated. The cumulative distribution function, or CDF, is defined as the probability that a random variable will be less than or equal to a given value. In this case, the random variable is the number of objects completed by the end of the lifetime. Therefore, the CDF can easily be calculated as $\left(1-\vec{R}(n+1)\right)$ for each value of *n*. First, from basic definitions, the probability that *x* is greater than a given value *n* can be determined using $\vec{R}(n)$:

$$\begin{aligned} &\text{By Definition :} \\ &P(x \geq n) = \vec{R}(n) \\ &\therefore \\ &P(x > n) = P(x \geq n) - P(x = n) \\ &P(x > n) = \vec{R}(n) - (\vec{R}(n) - \vec{R}(n+1)) = \vec{R}(n+1) \end{aligned} \tag{3-40}$$

The definition of the CDF is the probability that *x* is less than a given value *n,* or one minus the probability that *x* is greater than or equal to *n.* This is shown in Equation 3-41:

$$\begin{aligned} &P(x \leq n) = 1 - P(x > n) = 1 - \vec{R}(n+1) \\ &F(n) = 1 - \vec{R}(n+1) \end{aligned} \tag{3-41}$$

where *F(n)* is the Cumulative Distribution Function.

3.2.10 Approach Summary

The EPRA approach described above is summarized in Figure 3-15. Figure 3-15 is a distilled step-by-step guide to implementing the EPRA approach for any mission or project. Each of the steps shown is discussed in detail in the above sections. The seven main steps to the EPRA approach shown in Figure 3-15 are the same steps as the seven main boxes shown in Figure 3-1. The boxes labeled "adjustments," as well as other small details, are shown in the sub-steps in Figure 3-15.

1. Use probability of failures prior to operations to determine initial conditions and the expected value of the system parameters
2. Use Markov modeling to find **P**, a matrix of the probability of being in each state at each time-step
3. Find time to complete each object in all states
    1. Use productivity model
    2. Find proper order of objects
        1. If possible to complete object in any degraded state but not in nominal state, make time to complete object in nominal state equal to the shortest possible degraded state time
        2. Sort objects in terms of increasing time required to complete in nominal state
4. Find the expected time to complete each object. For each object:
    1. Find the index of the current simulation time, and the time to complete each object ($\vec{t}$)

    $$index = \frac{time}{\Delta t} \quad , \quad \vec{T} = \frac{\vec{t}}{\Delta t}$$

    2. Find the expected number of time steps to complete the object
        1. Use adjusted values of probabilities for degraded states if object is beyond $\vec{N}_{degraded}(i)$
            1. Determine the number of objects that could be completed in the given lifetime in each degraded state: $\vec{N}_{degraded}$
            2. Find P_adj using the A matrix and $\vec{P}_{o\_adj}$

            $$\vec{P}_{o\_adj} = \frac{\vec{P}_o}{1 - \vec{P}_o(n)}$$

            $$\vec{P}_{o\_adj}(n) = 0$$

            3. Use the entry from **P_adj** instead of **P** if the object is beyond $\vec{N}_{degraded}(i)$
        2. Normalize probabilities based on only those states in which completing the object is possible

        $$\vec{s}_f = find(\vec{t} \neq 0) \quad , \quad \vec{P}_n = \frac{\mathbf{P}(index, \vec{s}_f)}{sum(\mathbf{P}(index, \vec{s}_f))}$$

        $$E[T] = \overline{T} = \vec{T}(\vec{s}_f) \cdot \vec{P}_n$$

    3. Update clock by the expected number of time-steps

    $$time = time + \overline{T} \times \Delta t$$

    4. If time is less than the lifetime, move on to the next object

Δt = Length of one time-step

$\vec{P}_o$ = Initial conditions: Vector of probabilities of being in each state at beginning of life

A = State-transition matrix

$\vec{t}$ = Column vector of times required in each state. Reported as 0 if not possible to function in that state.

P = Matrix of the probability that the system is in each state (columns) at each time (rows).

$\vec{s}_f$ = Vector of states in which system is functioning. i.e. $\vec{t}(\vec{s}_f) \neq 0$.

$\vec{T}$ = Number of time-steps required in each state.

$R(i)$ = Probability of being in a working state when object i is completed

$\vec{P}_{exact}$ = Probability of completing exactly each number of objects.

$E[objects]$ = Expected number of objects.

$\sigma(objects)$ = Standard deviation

F = Cumulative Distribution Function (CDF)

$\vec{t}_e$ = Vector of expected times to complete each object

5. Calculate the $\vec{R}$ vector
    1. Define $\vec{R}(n)$ as the probability that the system is working when n objects are completed

       $\vec{t}_e(n)$ = Expected time at which object n is completed

       $$\vec{\mathrm{R}}(\mathrm{n}) = sum\left(\mathbf{P}\left(\frac{\vec{t}_e(n)}{\Delta t}, \vec{W}\right)\right)$$
    2. Adjust $\vec{R}(n)$ for situation in which it is only possible to complete the object in the first state
        1. Keep track of time to complete each object in first state. If object, and all objects after given object, can only be completed in first state, use probability that the system is still in the first state when reach given object.
    3. Adjust $\vec{R}$ to ensure calculating probability of completing n objects and not the first n objects in the order calculated.
        2. Sort $\vec{R}$ in decreasing order
    4. Adjust for situation in which objects that can be completed in the degraded states are late in the initial ordering

       $\vec{o}_{ds}$ = Vector of objects that can be completed in all possible states.

       $$\vec{\mathrm{t}}_{\mathrm{ds}}(n) = \sum_{i=1}^{n} \vec{T}\left(\vec{o}_{ds}(i)\right) \quad \text{if } sum\left(\mathbf{P}\left(\vec{\mathrm{t}}_{\mathrm{ds}}(n),:\right)\right) > \vec{R}(n)$$
       $$\vec{R}(n) = sum\left(\mathbf{P}\left(\vec{\mathrm{t}}_{\mathrm{ds}}(n),:\right)\right)$$
6. Find the vector of probabilities that the system completed exactly n objects before failing.
    1. Probability of completing exactly n objects is the same as the probability of being in a working state at the end of the nth object, but in a failed state at the end of the $(n+1)^{th}$ object.
        1. If system is not working at the end of the $(n+1)^{th}$ object, defined as $\left(1-\vec{R}(n+1)\right)$, one of two events must have occurred:
            1. The system failed prior to object n : $1-\vec{R}(n)$
            2. The system failed while completing object $n+1$ resulting in exactly n objects. Define this probability as $\vec{P}_{exact}(n)$

               $$\left(1-\vec{R}(n+1)\right) = \left(1-\vec{R}(n)\right) + \vec{P}_{exact}(n)$$
               $$\vec{P}_{exact}(n) = \left(1-\vec{R}(n+1)\right) - \left(1-\vec{R}(n)\right)$$
               $$\vec{P}_{exact}(n) = \vec{R}(n) - \vec{R}(n+1)$$
7. Determine the expected number of objects, the standard deviation, and the CDF

$$E[objects] = \sum_{n=1:length(objects)} n \times \vec{P}_{exact}(n) \qquad P(x \geq n) = \vec{R}(n)$$

$$E[objects] = \vec{P}_{exact} \times [1 \quad 2 \quad \ldots \quad n]' \qquad P(x > n) = P(x \geq n) - \vec{P}_{excact}(n) = \vec{R}(n) - \left(\vec{R}(n) - \vec{R}(n+1)\right)$$

$$E[objects^2] = \sum_{n=1:length(objects)} n^2 \times \vec{P}_{exact}(n) \qquad P(x > n) = \vec{R}(n+1)$$

$$\sigma(objects) = \sqrt{\left(E[objects^2] - (E[objects])^2\right)} \qquad P(x \leq n) = F(n) = 1 - P(x > n) = 1 - \vec{R}(n+1)$$

Figure 3-15: Step-by-step summary of EPRA approach

3.3 Testing the EPRA Approach

3.3.1 Test Set-up

As with most reliability and risk modeling, there is little to no data available to verify that the approach presented above is producing accurate results. In the aerospace industry, systems take years to be developed and built, during which time the final, actual productivity is unknown. Additionally, only a single copy of each system is usually built, providing only a single data point to judge the expected productivity. Therefore, the only available method to test the EPRA approach is to use simulation. A Monte Carlo simulation was used to test the results of the method discussed above.

At first glance, the probability that a particular failure did not occur in each time step in the Monte Carlo analysis may be calculated as $R = e^{-\lambda t}$, where t is the current time in the simulation and λ is the failure rate for each particular failure. However, this probability is the probability of no failure occurring anytime before the given time, t. In the Monte Carlo analysis the state the system is currently in is known. Therefore, the probability of particular failures occurring previous to that time step is zero, because if the failure had occurred, the system would be in a different state. What is really needed is the probability of the failure not occurring in that exact time step. Therefore, the correct equation for the reliability in that time step uses the amount of time in the time step, or Δt, instead of the current time. The correct equation for the probability of each particular failure not occurring in a given time step is $R = e^{-\lambda \Delta t}$.

This equation can be derived more rigorously from first principles. What is needed is R, defined as the probability that the system did not fail in a given time step. This is equal to one minus the probability that the system did fail in the given time step, defined as P^*. The fact that we are dealing with a given time step implies that the system did not fail before the beginning of the time step, but did fail before the end of the time step. Therefore, P^* can be defined rigorously as:

$$P^* = P(T \le t_2 | T \ge t_1) \qquad (3\text{-}42)$$

where T is the time a failure occurred, t_1 is the time at the beginning of the time step, and t_2 is the time at the end of the time step. In a general sense,

$$P(A|B) = \frac{P(AB)}{P(B)}$$
$$\textit{and} \qquad (3\text{-}43)$$
$$R(t) = P(T \le t) = 1 - e^{-\lambda t}$$

where $P(AB)$ is the probability of A and B both occurring, $P(B)$ is the probability of B occurring, $P(A|B)$ is the probability of A given B, T is the time a failure occurred (a random variable), t is a given time, and λ is the failure rate. Using this formula, P^* can be derived. Using Equation 3-42 and the first line of Equation 3-43:

$$P^* = P\left(T \le t_2 | T \ge t_1\right)$$
$$P^* = \frac{P\left(t_1 \le T \le t_2\right)}{P(T \ge t_1)} \qquad (3\text{-}44)$$

Next, the numerator can be simplified. Figure 3-16 provides a graphical description of this step. In this figure, the area shown with red stripes is the probability that X is less than x_2, called $F(x_2)$. The area shown with blue stripes is the probability that X is less than x_1, called $F(x_1)$. Additionally, the figure shows that the probability that X is larger than x_1 but smaller than x_2, shown as the area on the figure with red stripes only, can be calculated as $F(x_2)$- $F(x_1)$.

$$P^* = \frac{P\left(T \le t_2\right) - P\left(T \le t_1\right)}{P\left(T \ge t_1\right)} \qquad (3\text{-}45)$$

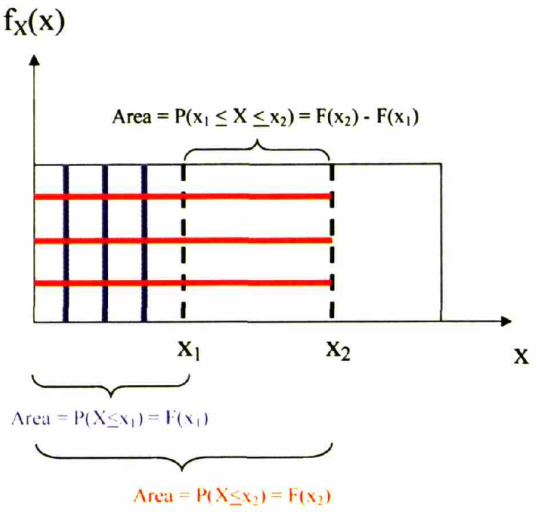


Figure 3-16: Clarification of $P(t_1<=T<=t_2)=P(T<=t_2)-P(T<=t_1)$

Combining Equation 3-45 with the second line of Equation 3-43:

$$P^* = \frac{\left(1-e^{-\lambda t_2}\right)-\left(1-e^{-\lambda t_1}\right)}{e^{-\lambda t_1}} \qquad (3\text{-}46)$$

Finally, simplifying and using the definition of the time step gives us the final formula for P^*, as shown in Equation 3-47:

$$\begin{aligned} P^* &= \frac{(e^{-\lambda t_1} - e^{-\lambda t_2})}{e^{-\lambda t_1}} \\ P^* &= 1 - e^{\lambda(t_1 - t_2)} \\ P^* &= 1 - e^{-\lambda(\Delta t)} \end{aligned} \qquad (3\text{-}47)$$

Since P^* is defined as the probability that the system will fail during the time step, R, or the probability that the system will not fail during that time step, is simply $1-P^*$, as shown in Equation 3-48.

$$R = 1 - P^* = e^{-\lambda(\Delta t)} \qquad (3\text{-}48)$$

Once the method for calculating R in each time step is determined, each trial of the Monte Carlo simulation can calculate the number of objects completed. This is accomplished by stepping through the simulation one time step at a time. Each trial begins in the completely functioning state. After testing for pre-operational failures, the probability of a failure not occurring during each time step is determined using the method described above. The Matlab function "rand" is used to draw a random number between zero and one. If this random number is larger than the calculated R, then a failure has occurred. The state of the system is changed to reflect the failure and, if the system is still functioning, the time required in that state to complete that particular object is calculated. Using the length of the time step and the completion time, the fraction of the object that is completed in that time step is calculated. The simulation then moves on to the next time step and repeats the process until either the system fails or the total fraction of an object is equal to one. Once an object is completed, the information required for the next time step is calculated using the characteristics of the next object in the list. This process is repeated until either the system has failed or the lifetime of the mission is exhausted. At the end of the simulation, the total number of objects completed is calculated by summing up the fractions of all objects in the list.

The path-dependent EPRA simulation approach discussed previously was tested against this Monte Carlo approach to verify the accuracy of the new method. All tests were initially conducted using 100 trials per Monte Carlo simulation. It should be noted that these tests are meant to validate the approach and not the specifics of the risk model used. Both approaches use the same model, and should therefore get the same or very similar results. However, there is nothing in these tests to validate that the model used is modeling the example mission correctly.

3.3.2 Results

The new EPRA path-dependant simulation approach was tested against the Monte Carlo simulation approach for two different models and many different scenarios. The first model, called the Detailed Level model, includes detailed failure modes for an example mission. The second model, called the Systems Level model, models the

degraded state productivities of several different architectures for the same mission, and includes major system-level failures only. The two simulation approaches were tested against one another using these models with several different scenarios. Different scenarios contained varying combinations of lifetime, time step, failure rates, system configurations and architectures.

Thirteen different scenarios were tested using the Systems Level model along with twenty-two scenarios using the Detailed Level model. The results from the two different approaches were then compared for each scenario. A p-test was completed for each scenario [Rumsey, 2003]. In these tests, it is hypothesized that the EPRA path-dependant simulation approach discussed above is correct and providing accurate answers. The p-value from this test gives the percentage chance that, if the true values were the same as the EPRA approach results, the Monte Carlo would return the given results. A p-value of five or higher is considered a passing value, leading to a 95% confidence in the hypothesis. See Figure 3-17 for an explanation of the p-value. In Figure 3-17, the blue line represents the Monte Carlo results for the number of objects. The red line represents the EPRA results for the expected number of objects. The shaded area shows the probability that the Monte Carlo results would have returned a value as far away or farther than the actual value returned, if the EPRA results are assumed to be accurate, which is defined as the p-value.

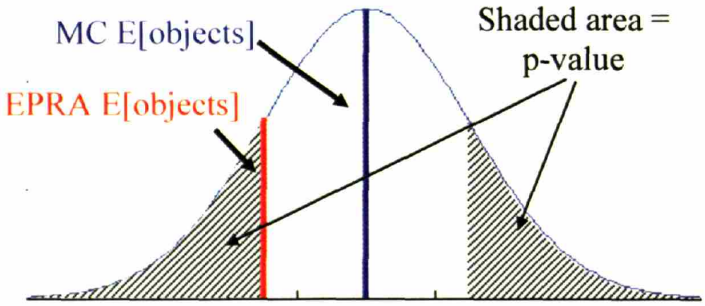
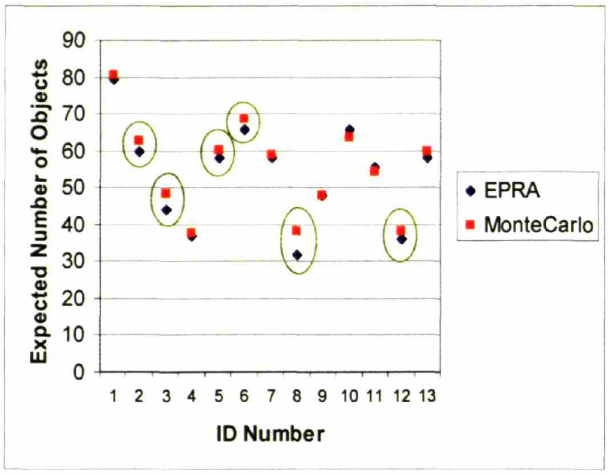


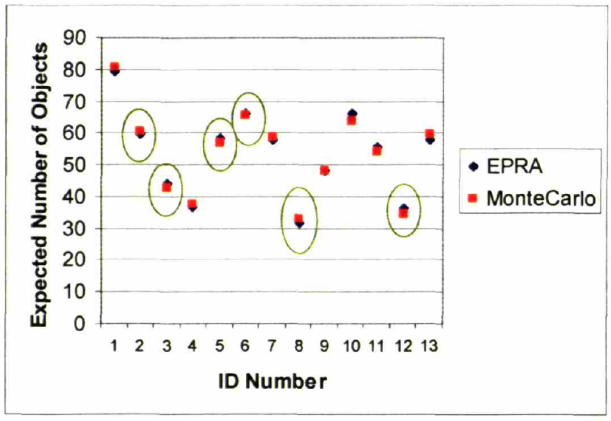
Figure 3-17: Explanation of p-value (two-tailed).

For both the Detailed Level model and the Systems Level model cases, a single scenario initially failed the p-test used to compare the two simulation approaches. This was a total of two p-test failures out of 35 trials. It is worth noting that this number of failures is to be expected. Recall that passing the p-test is defined by a having a 95% confidence in the hypothesis. Therefore, even in a perfect case, 5% of the results should fall outside this 95% confidence level and result in a failure in the p-test. Two failures out of 35 trials is a 5.7% failure rate, which is nearly exactly what would be expected given the nature of the p-test.

In addition to the one p-test failure, several scenarios from each model produced results that varied between the EPRA simulation and the Monte Carlo simulation by more than expected. In each case, when the scenario was run again with more trials in the Monte Carlo simulation, the results became much closer and passed the p-test. This is shown in Figure 3-18. These results show not only that the new EPRA approach does an excellent job of matching the Monte Carlo results, but also highlight one of the weaknesses of using Monte Carlo simulations. While using as few trials as possible per Monte Carlo simulation will help to keep down the simulation time, it can lead to errors and uncertainty in the results, since the Monte Carlo simulation is by definition dependent upon random chance. The new EPRA simulation approach is both quite accurate when compared to the Monte Carlo results and completely repeatable with the same accuracy level every time. The accuracy of the EPRA approach can be seen in Tables 3-1 and 3-2, and is discussed below.



a) Initial results



b) Results after re-running Monte Carlo simulations

Figure 3-18 : Results for different scenarios for the Systems Level model tests before and after re-running Monte Carlo simulations. The scenarios circled in green have been re-done with additional trials per Monte Carlo.

The numerical results of the simulation testing can be seen in Table 3-1 and Table 3-2. Table 3-1 shows the results for the Detailed Level model, while Table 3-2 shows the results for the Systems Level model. Note that in the best cases, the results from the Monte Carlo simulation and the EPRA simulation matched almost exactly. Even in the worst performing cases, the differences between the results from the two approaches are very small. This is best seen by noticing the fraction of a standard deviation (SD) that separates the two approaches, shown in the last three rows of Table 3-1 and Table 3-2. The standard deviation metric takes the standard deviation from the Monte Carlo

simulation to be "truth" and determines the ratio of the difference in the expected number of objects, between the Monte Carlo simulation and the EPRA approach, to this standard deviation. This metric has an average value of zero, to two significant digits, for both types of models. This implies that not only are the results nearly identical, the EPRA approach is not consistently either larger or smaller than the Monte Carlo approach. Even when looking at the absolute value of the difference between the approaches, the maximum difference found in either type of model is only 12% of a single standard deviation. These results clearly show that the EPRA approach is providing very accurate results.

Table 3-1: Performance results from Detailed Level model tests.

Number of Scenarios Tested	22
Average p-value	73.8
Min p-value	7.2
Max p-value	100.0
Average % off from MC	-0.27%
Min |% off from MC|	0.05%
Max |% off from MC|	5.8%
Average # of SD off from MC	0.00
Min |# of SD off from MC|	0.001
Max |# of SD off from MC|	0.12

Table 3-2 : Performance results from Systems Level model tests.

Number of Scenarios Tested	13
Average p-value	62.6
Min p-value	31.7
Max p-value	100.0
Average % off from MC	-0.16%
Min |% off from MC|	0.22%
Max |% off from MC|	5.28%
Average # of SD off from MC	0.00
Min |# of SD off from MC|	0.002
Max |# of SD off from MC|	0.06

The new EPRA approach is also capable of calculating the CDF of the expected productivity. This allows a designer to get a feel for where a requirement stands in relation to the probability of meeting that requirement. Examples of the CDFs calculated

by the EPRA approach compared to those calculated by the Monte Carlo simulation are shown in Figure 3-19. Note that the two CDFs follow the same trends and have break-points at the same locations for both approaches. Since the CDF shows the probability of meeting various productivity levels, providing an accurate CDF to design teams could be a powerful design tool.

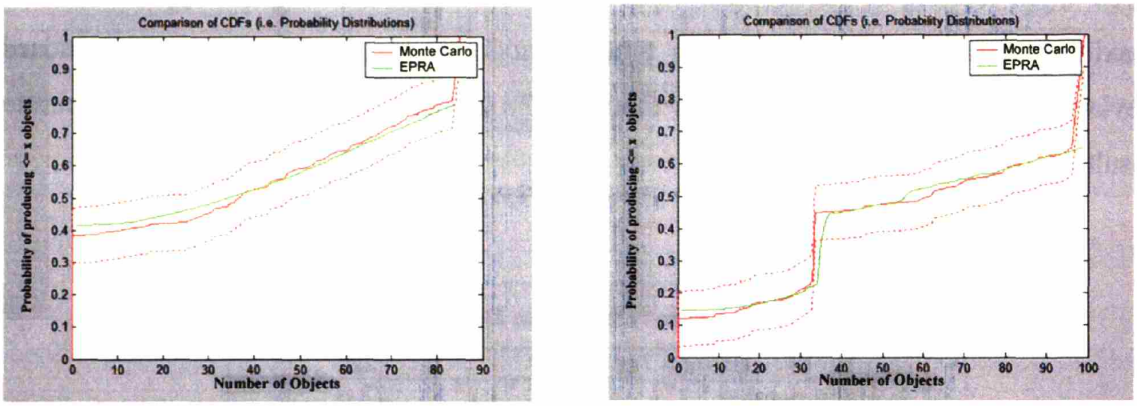


Figure 3-19 : CDFs for two different tested scenarios. The solid green line shows the new EPRA simulation results while the red lines show the Monte Carlo results (dashed lines represent the 95% confidence interval).

The minor differences between the EPRA and Monte Carlo results can be explained both by the randomness associated with the Monte Carlo result as well as by the approximations used in the EPRA approach. While these approximations will lead to a very small difference between the EPRA results and the truth-value, these small errors are justified by the speed of calculation. Table 3-3 and Table 3-4 show the computation times required for the new EPRA simulation versus the Monte Carlo simulation. On average the computation time was nearly 5 times faster for the Systems Level model cases and nearly 70 times faster for the Detailed Level model cases using the new EPRA simulation over the Monte Carlo simulation. Additionally, the maximum computation time over all scenarios was reduced from 2.5 hours for the Monte Carlo simulation to only a little over 10 minutes for the new EPRA approach. Note that while the code was not optimized to minimize computation times for either approach, effort was taken to ensure that neither effort wasted or repeated calculations.

Table 3-3 : Computation times for Detailed Level model tests. EPRA stands for the EPRA simulation and MC stands for Monte Carlo simulation.

Average EPRA Time	2.4 min
Min EPRA Time	0.5 min
Max EPRA time	3.1 min
Average MC Time	85.0 min
Min MC Time	21.4 min
Max MC Time	149.7 min
Average MC Time/EPRA Time	69.3
Min MC Time/EPRA Time	7.7
Max MC Time/EPRA Time	274.1

Table 3-4 : Computation times for Systems Level model tests. EPRA stands for the EPRA simulation and MC stands for Monte Carlo simulation.

Average EPRA Time	5.5 min
Min EPRA Time	1.6 min
Max EPRA time	11.2 min
Average MC Time	18.2 min
Min MC Time	8.1 min
Max MC Time	40.9 min
Average MC Time/EPRA Time	4.6
Min MC Time/EPRA Time	1.9
Max MC Time/EPRA Time	11.9

The computation times for the EPRA approach are longer for the Systems Level model than they are for the Detailed Level model. This is caused by the fact that differences in productivity for the Detailed Level model are based primarily on changes to factors applied to the nominal productivities. Therefore, the time required to complete each object only needed to be calculated once and could then be adjusted with a minimal calculation, to obtain the time required to complete the object in the degraded states. The differences in productivity between states in the Systems Level model are based primarily on new configurations; consequently, the time required to complete each object needed to be calculated separately for each degraded state for each object.

In an opposite trend from the EPRA approach, the computation time for the Monte Carlo simulation using the Detailed Level model takes longer than the Systems Level model, because it is necessary to calculate the actual time required for each object during each Monte Carlo run using the Detailed Level model. Unlike in the Systems Level model, failures can build on one another. It is possible to calculate the base

productivity times in advance, but initial productivity factors depend on starting conditions and all productivity builds off those factors, requiring that the final time, including both the factor and the pre-calculated base time, be calculated for each object. While this calculation is simple and takes little computational effort per object, the time and effort required to repeat this calculation for each object in each Monte Carlo trial builds up. This situation is more complicated, and in a sense a better approximation of reality, than the Systems Level model.

3.4 Conclusions

The new EPRA approach presented here uses small approximations to directly calculate the expected productivity, standard deviation of that productivity, and CDF of systems with path-dependant productivities. These values can then be used as metrics in any design trade matrix to facilitate decisions between designs. The new EPRA approach presented returns statistically identical results to those of a conventional Monte Carlo simulation, but calculates these results in significantly less time. This leads to the ability to test multiple designs and use these results to incorporate risk and degraded state productivity into the design.

Chapter 4

TERRESTRIAL PLANET FINDER INTERFEROMETER (TPF-I) OVERVIEW

The previous chapters discussed the value of using expected productivity as a risk metric, as well as the need for, and the development of, the new EPRA path-dependant productivity modeling approach. However, the clearest way to show that expected productivity analysis can have a true impact on design decisions is to show this impact through example case-studies using a real mission. The two case-studies presented in this thesis both use the same application mission: Terrestrial Planet Finder Interferometer (TPF-I). There are many reasons why TPF-I makes an excellent application mission for this research, including the fact that it is a very complex and expensive mission, it is currently in a very early phase of the design, it has very clear potential for degraded states, and, since it is an observatory, it has a path-dependant productivity function. The rationale for using TPF-I as the application mission for this research is explained in more detail at the end of this chapter; however, to give a better understanding of this rationale, as well as a better understanding of the models used in the case-studies, a mission overview and a discussion of how an interferometer works, both in general and in terms of the specific productivity model used, are given first.

4.1 Terrestrial Planet Finder Mission Overview

One of the fundamental questions in space science is whether or not life exists anywhere else in our universe. The possibility of life on other worlds has sparked the

imagination of scientists and the general public throughout the centuries. The concept of discovering that we are not alone is so exciting and thought provoking that it has spawned numerous books, movies, and television shows. The search for life on other worlds also has major scientific drivers. According to the 2001 decadal review of astronomy and astrophysics, published by the National Research Council:

> "The discovery of life on another planet is potentially one of the most important scientific advances of this century, let alone this decade, and it would have enormous philosophical implications." [JPL, TPF, 2005]

Due to the ramifications of the research involved, determining if life exists on other worlds is a one of the focus science areas of NASA. The program dealing with the search for other life is called Origins.

One of the flagship missions in the Origins program is called Terrestrial Planet Finder (TPF). TPF has two main goals [JPL, TPF, 2005]:

- Detect Earth-like planets in the habitable zone around other stars
- Characterize the atmospheres of the planets found to examine for evidence of possible past, current, or future life

The first goal of the TPF project is to detect Earth-like planets around other stars. For a planet to be considered "Earth-like" it needs to be approximately the same size as Earth. Planets that are either too big or too small are assumed to not be candidates for life. Additionally, the planets need to be located within the "habitable zone." The habitable zone is the range of distances from the star where it is assumed that life may be possible. If a planet is too close to or too far from a star, the temperature of the planet would not be appropriate to support life. Specifically, the habitable zone is set by the range in which the temperature of the planet could support liquid water. Science requirements state that TPF must survey 150 stars to look for planets in the habitable zone. All of these stars should be located within 15 parsecs of our solar system.

The second main goal of the TPF mission is to characterize any planets that are found during the detection phase of the mission. Spectroscopy will be used to determine

the chemical compositions of the atmospheres of any detected planets. The chemical composition of the atmosphere can give several clues about whether or not life has ever existed on the planet. Are the building blocks of life, such as water, carbon monoxide, or carbon dioxide present? Are there indications that life may currently exist on the planet, such as ozone, molecular oxygen, or non-equilibrium conditions? Information about the atmospheric content of any detected planets could be the first step towards concretely identifying life on another world.

The requirement that TPF must not only be able to detect planets within the habitable zone, but also characterize their atmospheres, presents the major technical hurdle for the mission. While planets have been detected around other stars in the past, none have been in the habitable zone. Indirect detection, such as detection based on gravitational wobbles, usually detects planets that are much closer to the star than the habitable zone definition allows. In addition, planets do not produce light of their own, but simply reflect the light of their parent star. This implies that planets themselves are very faint sources, making direct detection very difficult. In order to characterize the atmospheres of the planets that are found, the detection must be a direct detection. Direct detection of planets within the habitable zone is very difficult due to the relative brightness of the star compared to the planet. In general, the parent star is anywhere between one million and ten billion times brighter than the planet [JPL, TPF, 2005]. This problem is explained on the TPF website:

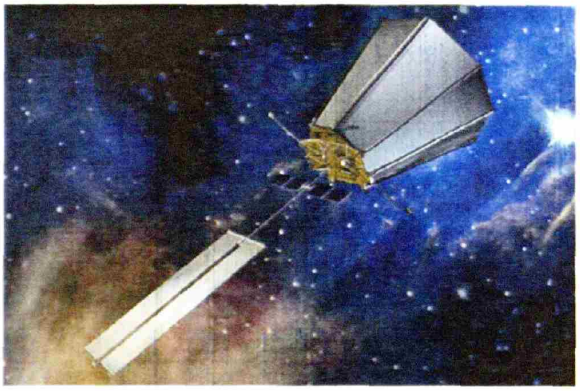
> "For example, if there were a planet orbiting Proxima Centauri, the nearest star, it would be 7,000 times more distant than Pluto. Trying to observe this planet would be like standing in Boston and looking for a moth near a spotlight in San Diego." [JPL, TPF, 2005]

A planet can be located by reducing the ratio of the brightness of the parent star to the planet. This is accomplished by reducing the light source from the star. Reducing the light source from the star is called blocking out the starlight, and is carried out using one of two technologies – coronagraphs or nulling interferometers.

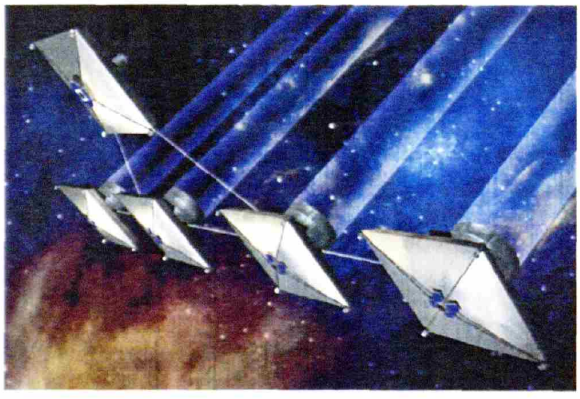
TPF will consist of two separate missions. The first mission launched will be a coronagraph instrument. The basic idea behind a coronagraph is to block out the parent

starlight by using an occulting disk. The occulting disk is flown in front of the telescope. The coronagraph version of TPF, known as TPF-C, is a visible light instrument.

The second TPF mission will be a formation flown nulling interferometer mission, known as TPF-I. While TPF-C is a visible light instrument, TPF-I is an infrared instrument. The difference in the wavelengths used is the main reason for including both missions in the TPF suite. The two different wavelength regimes can provide different and unique information from a spectroscopic analysis. The combination of the information provided by both wavelength regimes is exceptionally valuable when attempting to identify life signatures. Artist renditions of both TPF-I and TPF-C can be seen in Figure 4-1.



a. TPF-C



b. TPF-I

Figure 4-1: Artist renditions of both TPF missions

TPF-I uses a nulling interferometer instrument. A nulling interferometer combines light beams in a way such that some of the light cancels out, while other light is not cancelled out. The waves of light from the star are combined from different sources, or apertures, in a destructive way. In this way the light from the star is cancelled out. However, the light from the off-center planet is not completely cancelled out. To achieve the nulling interferometer functions most efficiently, TPF-I uses a formation of separate spacecraft. Either three or four apertures are flown in formation and used to collect the starlight. The starlight beams from these separate apertures are then transferred between spacecraft to the combining bench.

The research presented in this thesis uses TPF-I as the application mission for both case-studies. Therefore, the productivity model used, in addition to the rules for degraded state functionality, deals with the basic concepts of interferometry. To aid in better understanding these models, the concepts of interferometry in general, and of nulling interferometry, are explained further in the following section.

4.2 Basic Concepts of Interferometry

4.2.1 General Interferometry

Resolution is one of the key parameters used to describe the power of a telescope. A telescope with course resolution can make out smaller objects than one with fine resolution. This parameter improves (decreases) with increased diameter of the main aperture, or mirror. As mirrors get larger however, they get more impractical to launch into space. An interferometer is a type of telescope that uses multiple smaller mirrors instead of one large one. With this method, if two one-meter diameter mirrors are placed a kilometer apart they will have the same resolution as a one-kilometer diameter mirror. This method of improving resolution is very powerful for space-based telescopes, since launch costs can be dramatically reduced.

4.2.1.1 Fringes

A telescope creates images by collecting photons from the target being observed. In celestial observations the targets are usually stars. If it is sufficiently far away, a star can be considered a point of light with no angular diameter. A typical optical telescope with a single main aperture collects photons in the manner shown in Figure 4-2. In this figure, the black line is the photon rates from a single point of light, represented as the black dot. If a second point of light is next to the initial point of light, as in the green dot, it will create a similar pattern, slightly shifted, as seen by the green line. In this case the second, or green, point of light is fainter than the first, or black, point of light. This can be seen from the relative amplitudes of the peaks. The actual data from the telescope would not show these individual patterns, but the sum of the individual patterns. The angular resolution of a single aperture optical telescope is given by Equation 4-1.

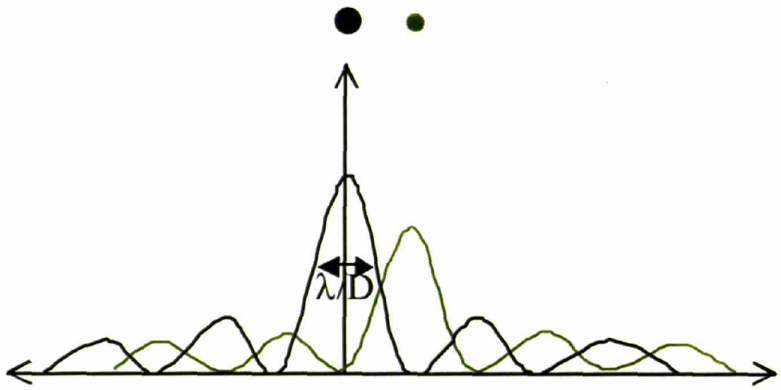


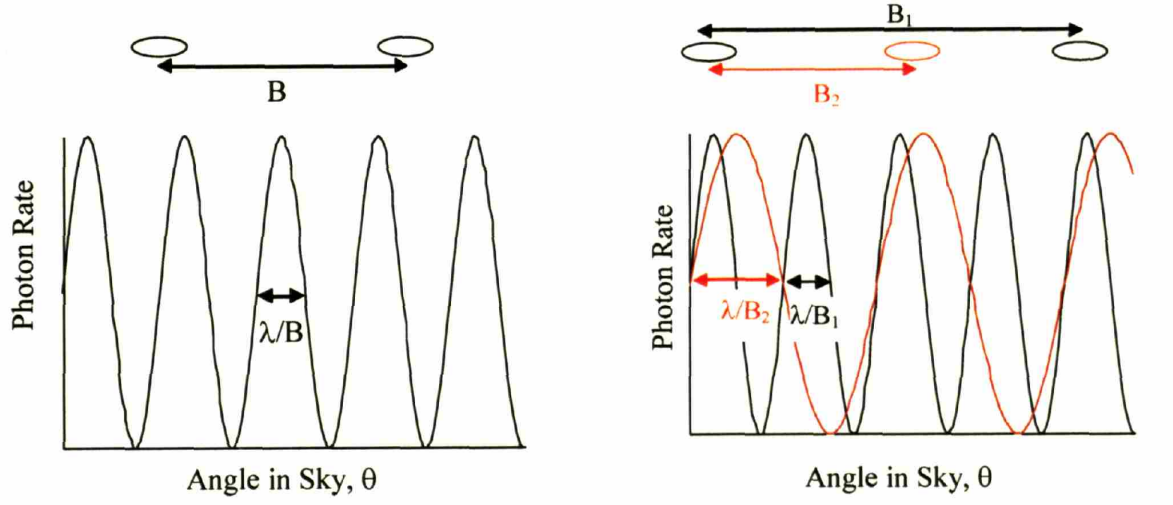
Figure 4-2: Photon rates for a single aperture optical telescope

$$\text{Angular Resolution} \approx \frac{\lambda}{D} \qquad (4\text{-}1)$$

In Equation 4-1, λ is the wavelength of the light being observed, and D is the diameter of the main aperture. If the second point of light is too close to the first point of light, then the peaks will overlap, and the telescope will not be able to see a distinction between the points. The second point, or star, needs to be separated from the first point, or star, by the

width of the peaks in order for the stars to be distinguishable. This gives the equation for angular resolution.

Interferometers are similar to single aperture optical telescopes in many ways. The images are again created by collecting photons from the targets. With interferometers, a number of measurements are required to get a full image of a target. An example of the data an interferometer would measure can be seen in Figure 4-3a. This pattern of photon rate versus projected angle in the sky is called a fringe, and is used to determine information about the target. The distance between the two collecting apertures is known as the baseline, and is represented as *B*. The pattern in Figure 4-3a is similar to that from an optical telescope, shown in Figure 4-2, in that the peaks are of equivalent widths, with the diameter simply replaced by the baseline. The main difference is that the peaks in the pattern from the interferometer do not decay, but rather are of constant amplitude. The effect of the baseline can be seen in Figure 4-3b. As the baseline increases, the frequency of the fringe increases. The amplitude of the peaks is again dependent on the magnitude of the target.



a: Single baseline **b. Showing the effects of varying baselines**

Figure 4-3: Photon rates for an interferometer

Interferometers use active delay lines to change the distance the light travels to the combining optics from one aperture versus the other aperture. When the light from the two apertures is combined, it creates the pattern shown in Figure 4-3. If the light

from the two apertures traveled exactly the same distance, or exactly one wavelength different, then it would combine constructively, giving rise to one of the peaks shown in Figure 4-3. If the light from the two apertures was exactly half a wavelength off, it would combine destructively, and give rise to one of the valleys shown in Figure 4-3.

There are two ways to think about the axes of a fringe. A fringe can be thought of as a projected pattern on the sky. In this method, the light from a target travels the same distance to both apertures if it is directly in line with the middle point of the two sets of optics, giving rise to a peak. As the star moves to one side or the other of the middle point, the light begins to travel slightly different amounts to each aperture, causing varying constructive and destructive interference levels, and giving rise to a fringe pattern. In this case, the x-axis of the fringe is the angle in the sky of the target compared to the mid-point of the apertures, and the y-axis remains the photon rate. Figure 4-3 shows this method of portraying a fringe, while Figure 4-4 shows an example of this angular offset. The second method of portraying a fringe is to consider a fringe the pattern a target would make in the focal plane of the instrument. In this method, the x-axis is the amount of offset in the delay line, or the optical path difference (OPD), and the y-axis is the photon rate. If this method of portraying a fringe is used, the pattern remains similar to the one shown in Figure 4-3; however, the axes change and the width of the peaks is no longer λ/B, but rather the distance between the peaks is simply λ, as shown in Figure 4-5. The patterns shown in Figures 4-3 and 4-5 are representative of a single point in the sky with zero angular width. [Lay, 2001]

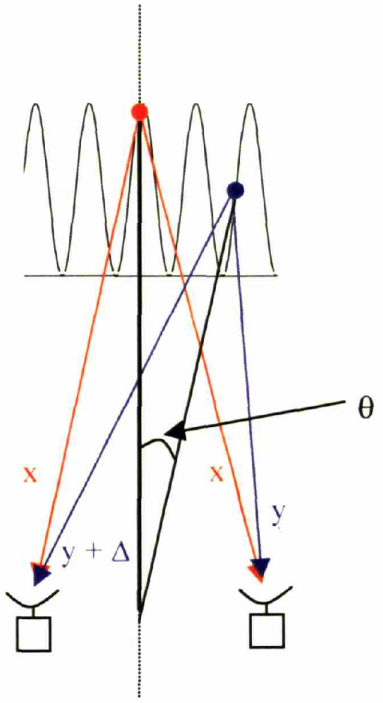


Figure 4-4: Definition of angle in sky

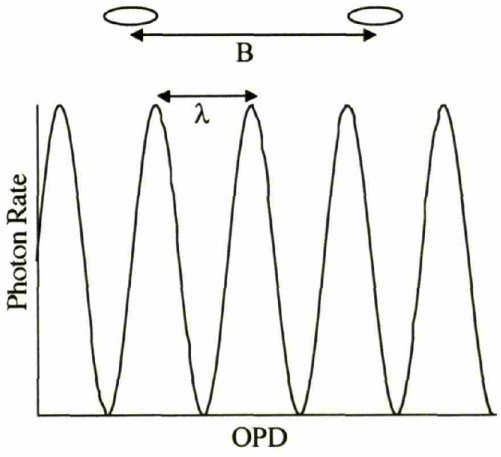


Figure 4-5: Photon rates for an interferometer

4.2.1.2 Visibility

Unless a star is infinitely far away, it is actually wider than a single point in the sky. This width is effectively seen in interferometer measurements as individual points

of light next to each other that together are as wide as the actual star. This can be seen in Figure 4-6.

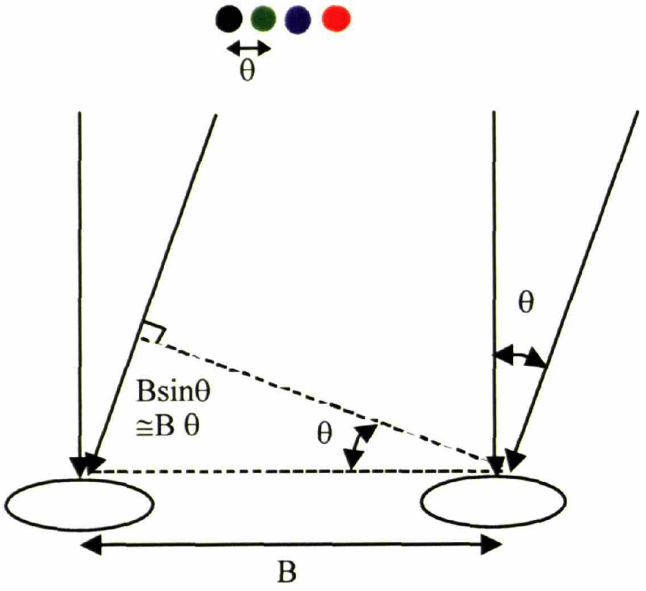


Figure 4-6: Collecting light from multiple points in an interferometer

In Figure 4-6, each point is separated by an angular distance θ. Note that the different colors in Figure 4-6 represent different points of light, all with the same wavelength. Light coming straight into both apertures is compared to light coming in at an angle θ, implying the target is offset in the sky by this same angle. This offset causes the light to travel $Bsin\theta$ farther to one aperture than to the other. This extra distance can be approximated as $B\theta$ for small angles. The effect on the fringe pattern is similar to the effect of adding a second point to the pattern in an optical telescope. This effect can be seen in Figure 4-7. A target represented by the four points shown in Figure 4-6 would be 4θ wide. As the star gets wider and wider, there are more and more points of light next to each other. As with the optical telescope, these individual patterns for each point do not appear in the data, but rather the sum of all photons is recorded. The sum of the individual patterns can be seen in Figure 4-8 for a single point of light up to four points of light. Note that as more points of light are summed, implying a larger star, the total photon rate becomes more constant, with less relative difference between the valleys and

the peaks. It is this difference that is used to measure the angular size of the star in the sky.

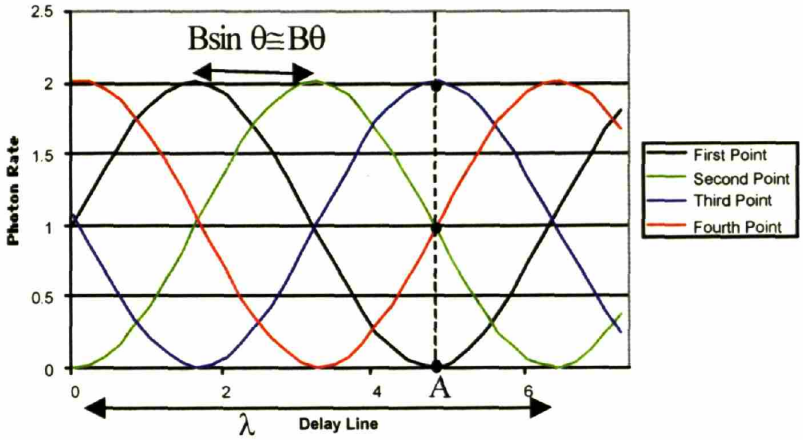


Figure 4-7: Photon rates from multiple points of light

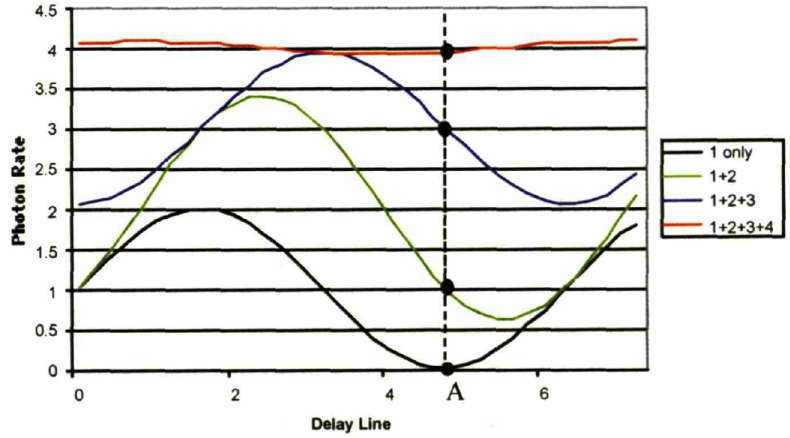


Figure 4-8: Total photon rates for up to 4 points

Visibility is a parameter used to measure the relationship between peaks and valleys of a fringe. Figure 4-9 and Equation 4-2 illustrate the method of calculating fringe visibility. If a single point of light is measured, as in the black line in Figure 4-8, the valleys of the pattern have zero amplitude. Therefore, the y variable in Equation 4-2 is zero, and the visibility is equal to one. However, if two or more points are seen to together, as in a star with angular width, the valleys no longer have amplitudes of exactly zero. For example, in Figures 4-6 and 4-7 the point A has zero photon rate if just the

black line is measured. If multiple lines are summed, as is the case with the green, blue, and red lines in Figure 4-8, the sum is no longer zero. These summed lines in fact will never reach a value of zero. Therefore, the value of y in the equation for visibility will no longer be zero, and the visibility will no longer be one.

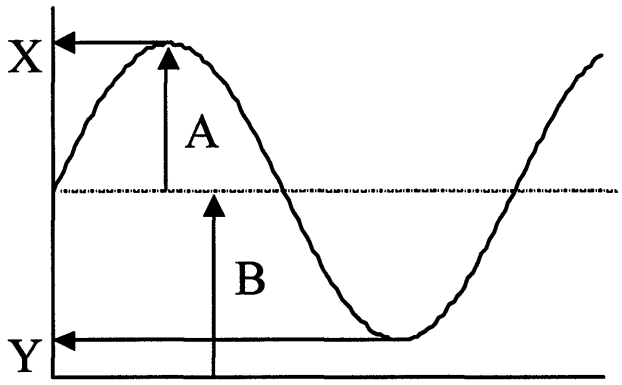


Figure 4-9: Visibility calculation definitions

$$vis = \frac{A}{B} = \frac{0.5(x-y)}{0.5(x+y)} \qquad (4\text{-}2)$$

As more patterns are summed the relative sum of the peak and the valley, B, increases, while the relative difference, A, decreases. This causes the visibility to decrease. In the extreme case, if the fringe were a constant value, x would equal y in Equation 4-2, and the visibility would be zero. Therefore, a single point of light will have a visibility of exactly one, while a star of infinite width will have a visibility of zero. This relationship can be seen in Figure 4-10.

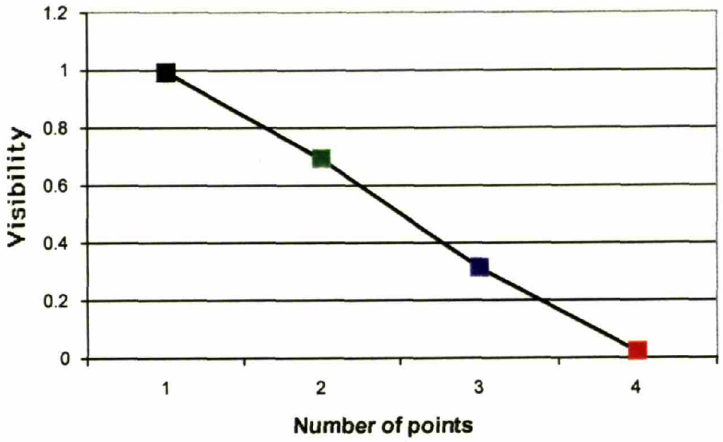
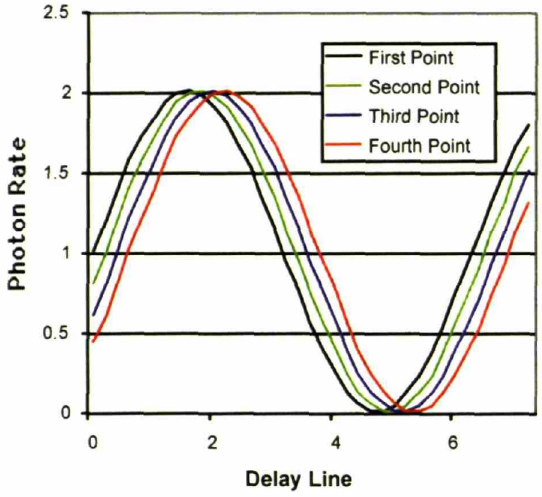
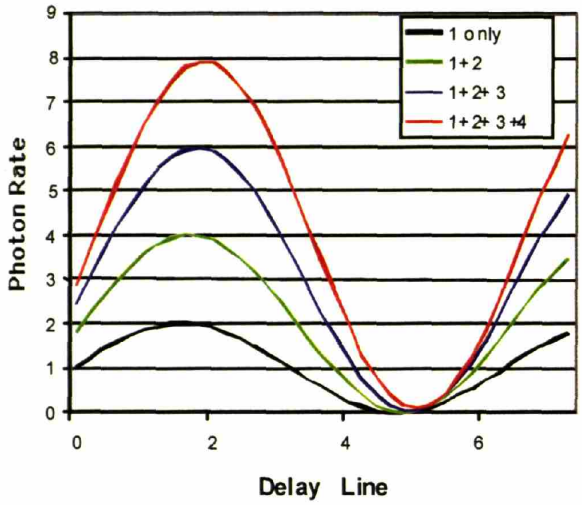


Figure 4-10: Visibility comparison for up to 4 points

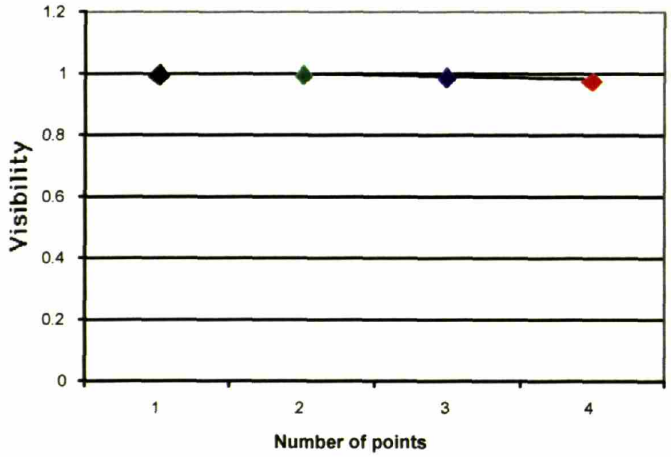
As discussed previously and shown in Figure 4-7, the distance between the patterns of individual points of light goes approximately as the baseline times the angular distance between the points. Therefore, as the baseline decreases, so does the distance between patterns in Figure 4-7. If this distance becomes too small, then it becomes impossible to distinguish between the peaks. This is similar to angular resolution of a single aperture optical telescope. If these patterns are too close, the visibility will not drop, since the pattern of the individual points summed up still approaches zero. This effect can be seen in Figure 4-11. Compare Figure 4-11 to Figures 4-7, 4-8, and 4-10 to see the difference between a large $B\theta$ and a small $B\theta$.



a. Photon rates



b. Total photon rates



c. Visibility Comparison

Figure 4-11: 4 points separated by 0.2 units (Figures 4-7, 4-8, and 4-10 are separated by 1.6 units)

Assuming an ideal instrument, visibility is always equal to one for a single point of light, and for a star of any width if the baseline is very small. As the baseline increases, the visibility drops. A sharper the drop in visibility implies a larger angular width of the star. As the baseline increases past the first minimum in visibility, the visibility begins to increase again. This effect could be seen by adding more points to the example shown in Figures 4-7, 4-8, and 4-10. A fifth point would add a second line

basically on top of the black line in Figure 4-7 and double the component from the first, or black, point in the sum. This would cause a larger visibility than if each component is only counted once, as shown. These later peaks in visibility are much smaller than the first peak however, and will eventually taper out to zero. This can be seen in Figure 4-12.

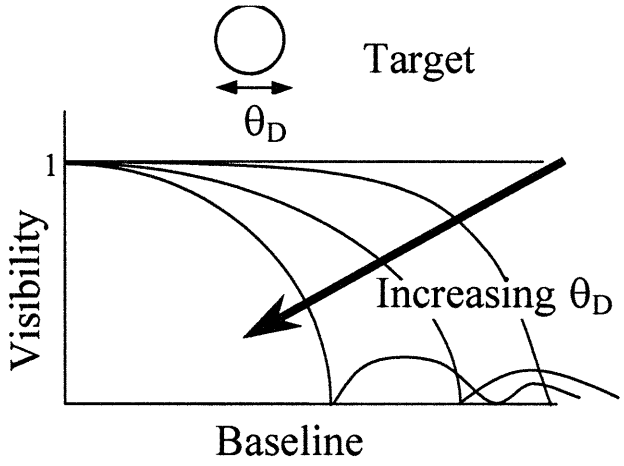


Figure 4-12: Relationship between visibility, baseline, and target size

Figure 4-12 is simply an example of the trends of visibility in relation to the angular width of the target and the baseline of the interferometer. Curves similar to those in Figure 4-12 exist with the exact relationship between these three parameters. Therefore, the size, or angular width, of a star, if it is assumed to be circular, can be measured by simply measuring the visibility of the target at one known baseline. The measurement can then be fit to one of the pre-existing curves to determine the size of the target.

Visibility can be measured by measuring the photon rate, N, at any four points along a wavelength in the fringe. This can be seen in Figure 4-13 and Equation 4-3.

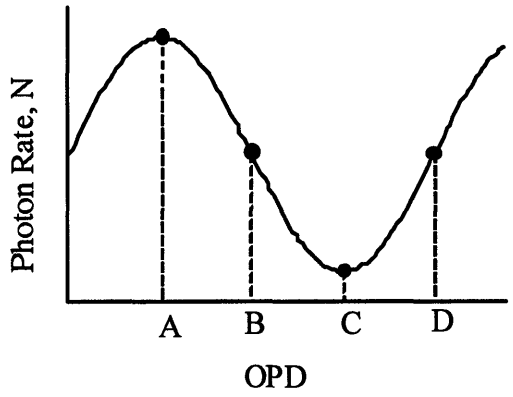


Figure 4-13: Visibility calculation definitions

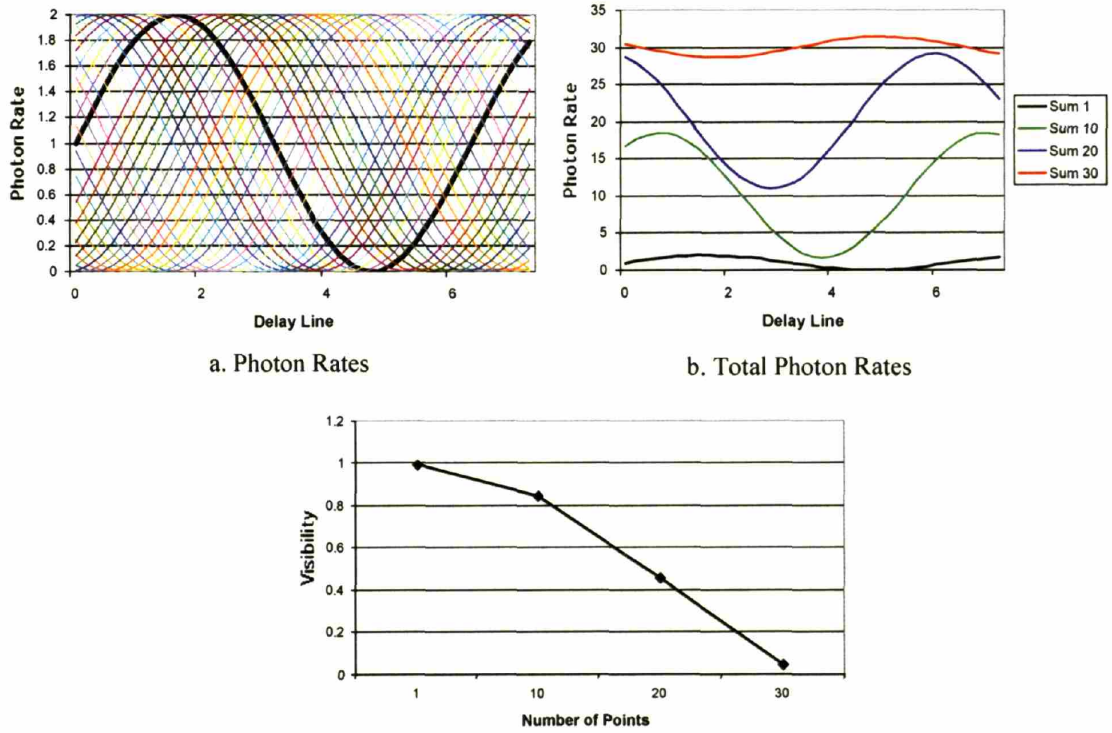
$$vis^2 = \frac{(N_A - N_C)^2 + (N_B - N_D)^2}{(N_A + N_B + N_C + N_D)^2} \qquad (4\text{-}3)$$

Figure 4-13 shows points *A*, *B*, *C*, and *D* falling directly on, or half way between, the exact peaks and valleys of the fringe. This does not need to be the case for Equation 4-3 to hold. The point *A* can be anywhere along the fringe. The points *B*, *C*, and *D* simply need to be measured relative to the point A, at exactly one-quarter wavelength intervals. Therefore, once the fringe is found for a given target, the visibility can be calculated from four measurements along that fringe. [Lay, 2001]

4.2.1.3 Resolution

As mentioned previously, a star or target with angular width can be thought of as individual points of light next to each other for a distance equal to the angular width of the target. If enough of these points are next to each other, the entire area within the pattern shown in Figure 4-7 will be filled in. This can be seen in Figure 4-14a. If the pattern is entirely filled in, there is no way to make out even a small fringe in the total photon rate, which approaches a constant value. This can be seen in Figure 4-14b. If the total photon rate is constant, then the visibility is exactly zero, and the interferometer cannot resolve anything. This is known as resolving out a star. This occurs if the

baseline times the angular width of the star (the distance between the first pattern's peak and the last pattern's peak – see Figure 4-7) is much greater than the wavelength of the light being observed. Therefore, it is difficult for an interferometer at a given baseline to resolve a star that has a larger angular width than the wavelength of the light divided by the baseline. If the angular width of a target is larger than this angle, the interferometer can only decipher that the target is larger than its capability to see, but cannot decipher any information on how much larger the target is. The angular width at which a star is resolved out is given in Equation 4-4. Note that in order to resolve individual targets of large angular width, a baseline should be small.



a. Photon Rates

b. Total Photon Rates

c. Visibility Comparison

Figure 4-14: Example of a resolved out star - 30 points separated by 0.2 units

$$\theta_{RO} >> \frac{\lambda}{B} \qquad (4\text{-}4)$$

There remains the question of how close together two individual targets can be for an interferometer to be able to distinguish between them. For example, how close can the two stars, or point sources, in a binary system be, before the interferometer sees them as a single point source? A binary system would create a visibility pattern similar to that shown in Figure 4-15. The first star would create the usual pattern shown in Figure 4-3a. The second star would create the same pattern, shifted over by an amount equal to the baseline times the angular separation between the two sources. When this shift is exactly equal to one-half the wavelength of light, the two patterns will add together and cause complete destructive interference. In other words, the total photon rate would be constant, causing a visibility of zero. This accounts for the null at lambda over two times the angular separation, shown in Figure 4-15. As the separation between the patterns continues, this process continues and eventually, when the baseline times the separation of the sources is equal to exactly one wavelength, the two patterns have complete constructive interference, and the visibility is once again one. In order to determine that there are two sources and not simply one larger source, the baseline must be able go past this null and see the second maximum peak in Figure 4-15.

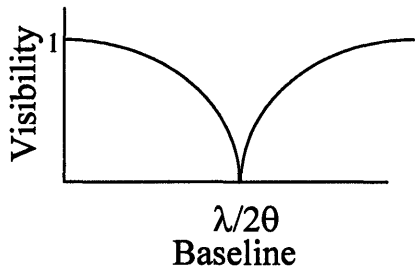


Figure 4-15: Visibility for a binary system

It is also possible to look at the angular resolution of an interferometer in a similar manner to the discussion of the angular resolution of a single aperture optical telescope. If the patterns in Figure 4-7 are too close together, as in Figure 4-11, then they cannot be distinguished from one another. One criterion for when peaks can be distinguished is that

the peak of the second pattern cannot be within the distance from the peak to the trough of the first pattern. For a square target, in which all the light has the same distance to travel, the first trough is at one half the wavelength. This is the easiest concept to visualize and has therefore been used in all previous discussions. For a circular target, the first trough is actually at approximately 1.22 times the wavelength, since there are more photons coming from the exact center of the target than from the sides. This can be seen in Figure 4-16.

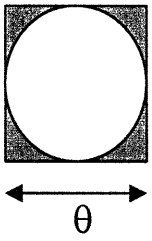


Figure 4-16: Difference between a circular target and a simpler to model square target

All of these arguments put the smallest angular separation at which an interferometer at a given baseline can still make out two individual targets between the wavelength over the baseline and the wavelength over two times the baseline. This can be seen in Equation 4-5. The range in this equation is due to the fact that there is no strict value of where the instrument can specifically separate two targets. The area in which it can and cannot separate targets blends together smoothly, and where exactly the cut-off is can be unclear or undistinguishable.

$$\frac{\lambda}{2B} \leq \theta_{RES} < \frac{\lambda}{B} \qquad (4\text{-}5)$$

It is worth noting that in order to resolve individual large targets (large θ_{RO}) a small baseline is needed (see Equation 4-4), but in order to resolve between two close small targets (small θ_{RES}) a large baseline is needed (see Equation 4-5). With a large

baseline, details of an image can be resolved, but the background and large areas in the image would be resolved out. With a small baseline the large areas and backgrounds can be resolved, but no detail would come through. This is one reason that any interferometer attempting to image a target needs a variable baseline. [Lay, 2001]

4.2.1.4 Imaging

In addition to the size of a target, an interferometer can also be used to gather information about the shape of a target. Figure 4-17 illustrates this process. If a target is actually an ellipse, rather than a circle, then the size information given by an interferometer with collecting mirrors horizontally across from one another would be different from the size information given by the same interferometer with the same baseline, but with the collecting mirrors vertically across from one another. This difference in measurements implies that the target is elliptical in shape. Therefore, an interferometer can begin gathering data on the shape of a target with just two measurements.

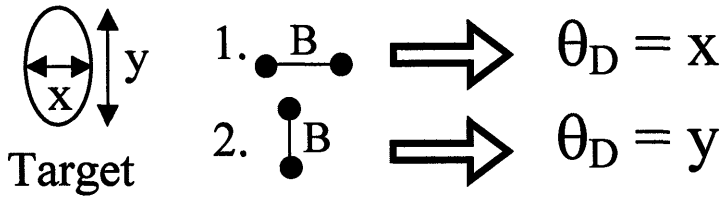


Figure 4-17: Resolving a target's shape

The two measurements shown in Figure 4-17 are represented by the red dots in Figure 4-18. The plane in Figure 4-18 is known as the UV-plane. Each measurement taken at a given baseline and orientation produces one UV-point. If the entire UV-plane is filled in, within a circle with a radius of the largest baseline used, a fully sampled image can be created. The transformation from the UV-plane to the image plane is

accomplished through a Fourier transform. With one point, the size can be determined. With two points, similar to the two red points in Figure 4-18, the basic shape can begin to be determined. With the entire plane filled in uniformly, as in the black dots in Figure 4-18, the entire shape of the target can be determined, and an image can be taken. The change in angle around the circle is used to gather shape information, and the change in radius through the circle is used to gather both detailed and large area information, as was discussed above. [Lay, 2001]

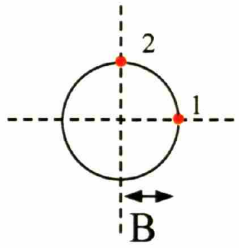


Figure 4-18: Sample UV-plane

4.2.1.5 Broadband Light

The previous discussion has involved a simplification to assist in the visualization of concepts. The light discussed above is assumed to be monochromatic, or single wavelength. While this simplification makes interference and other concepts much simpler to visualize, it is almost never physically realizable or useful. In reality, most light being studied by an interferometer has components of different wavelengths. When this occurs, it is impossible to get a visibility of exactly one. This is due to the fact that even if one component were shifted by exactly one wavelength, that shift would not be exactly one wavelength for a different component. In other words, the instance in which the optical path difference is exactly zero is the only instance in which all the light from both sides lines up exactly. At any other optical path difference other than zero, the light from at least one wavelength component will not be lined up exactly from the two apertures. This implies that the pattern the interferometer will receive for broadband light will have a maximum when the light is completely constructively interfered. The general pattern, as the OPD is increased and decreased, will remain the same as with

monochromatic light in the sense that it will still vary between peaks and valleys. However, the peaks will continuously decrease in magnitude, while the valleys will never be zero and will continuously increase in magnitude. This pattern can be seen in Figure 4-19. The visibility, as defined in the previous discussion, of broadband light is measured at the center of the fringe, using the first (zero-point) peak and valley amplitudes.

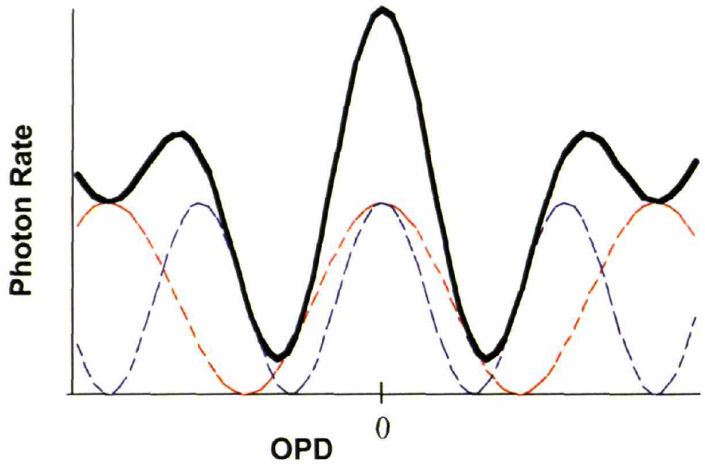


Figure 4-19: Photon rates for broadband light. The red and blue lines are individual wavelength components and the black line is the sum.

Figure 4-19 implies that the theoretical limit on visibility for broadband light is not one, but a value lower than one, since the first valley will never be zero. The specific theoretical limit is different for different combinations of wavelengths. For example, white light is comprised of a component of every wavelength. The photon pattern an interferometer would record for a point of pure white light would then be an impulse at zero OPD, with an amplitude dependant on the magnitude of the light being observed. At any point other than zero OPD, the photon rate would average to a constant amplitude equal to one half the amplitude of the impulse. This pattern can be seen in Figure 4-20, and is simply an extreme case of the pattern shown in Figure 4-19. If these numbers are

plugged into Equation 4-2, the theoretical limit on visibility for white light is shown to be one-third. This calculation is shown in Equation 4-6. [Miller, 2001]

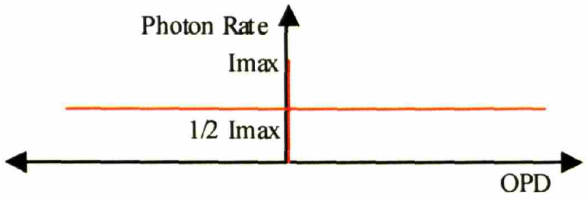


Figure 4-20: Photon rate for white light

$$\text{max visibility} = \frac{\frac{1}{2}(I_{max} - \frac{1}{2}I_{max})}{\frac{1}{2}(I_{max} + \frac{1}{2}I_{max})} = \frac{\frac{1}{2}}{\frac{3}{2}} = \frac{1}{3} \qquad (4\text{-}6)$$

4.2.2 Nulling Interferometry

In nulling interferometry, a π phase shift is added to one of the light beams. This causes destructive interference at the center of the source, in this case the star. The same concept of fringes that is used in general interferometry is also used in nulling interferometry. Figure 4-3 is still appropriate for nulling interferometry; however, now the null of the fringe is located at the zero point in terms of angle on the sky. This is shown in Figure 4-21.

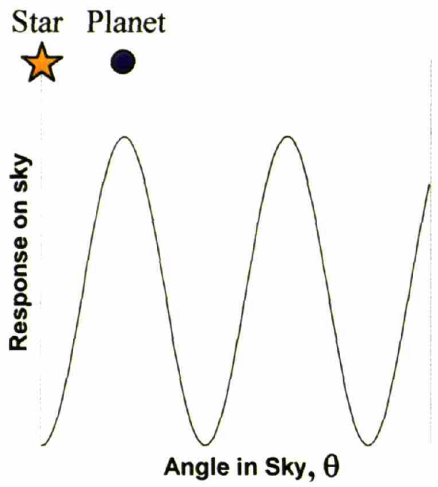


Figure 4-21: Nulling interferometer fringes

If the star is located in the null of the fringe, it is possible to detect a planet located in one of the peak areas of the fringe. If the baseline is kept at a single orientation, the signal received will be a steady value of a combination of signal received from the planet, stellar leakage from the edge of the null, and other noise sources. In this situation, it would be impossible to determine how much of photons detected, if any, are from a planet as opposed to from the other sources. If the baseline is rotated however, the planet will move across the fringes. As the planet moves into and out of the nulls and peaks of the fringes, the photons received from the planet will modulate, as shown in Figure 4-22 [Henry, 2003]. Therefore, if a planet is located in the habitable zone of a star, the total photon count will modulate as the instrument is rotated. The difference between the peaks and valleys of this photon modulation indicates the photon flux of the star.

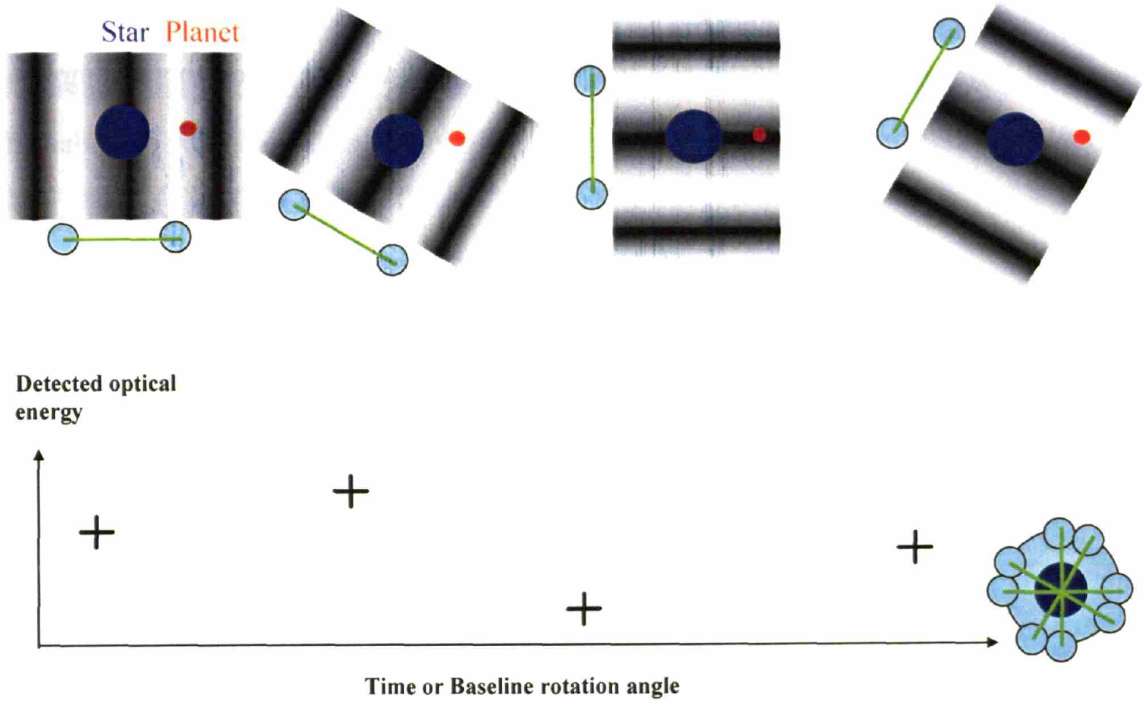


Figure 4-22: Detecting a planet using nulling interferometry

In nulling interferometry, the path-lengths from the two apertures need to be exactly equal, and the apertures need to be pointed at the exact middle of the star. This places the null at the proper location to block out the starlight, without blocking signal from the planet. To keep the path-lengths equal and the star centered in the field of view, a second detector, known as the fringe-tracking camera, is used. For this detector, the π phase shift is not added to either light path. Therefore, this detector records photon rates similar to those shown in Figure 4-3a. As discussed previously, the x-axis of interferometer fringes can be viewed either as OPD, or as the angle in the sky of the light source. If the x-axis is the angle on the sky of the star, by tracking the photon rate in the fringe tracking camera the instrument can control the location of the star in the field of view. Additionally, if the x-axis is thought of as the OPD, tracking the fringe ensures that the path-lengths of the light to each aperture are identical, or that the OPD is zero. Therefore, by using the fringe tracking camera, a nulling interferometer can ensure a null by keeping the path-lengths equal, and can keep that null on the center of a star such that

any planets can be detected. The basic concept of using two detectors for nulling interferometry is shown in Figure 4-23. Note that Figure 4-23 is a concept diagram, and the actual beam combining paths and instrument design will be much more complex. [Lay, August 2005]

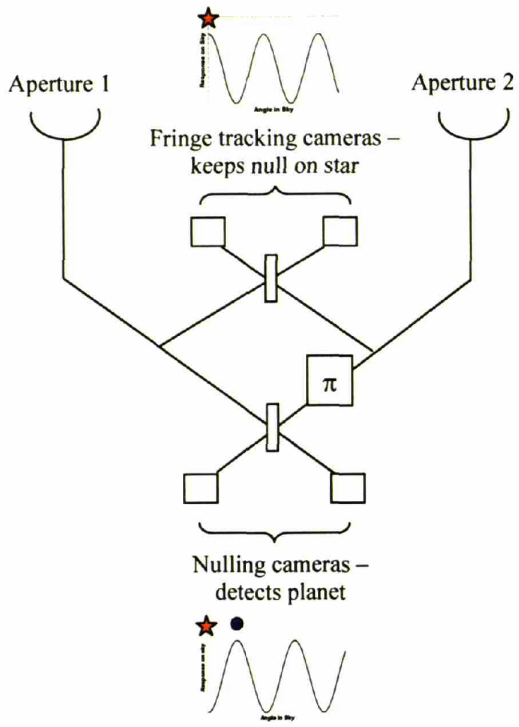


Figure 4-23: Concept of nulling vs. fringe tracking detectors

4.3 Star-count Model

The productivity model used to analyze the performance of various TPF-I architectures is called the star-count model. This model was originally written by Serge Dubovitsky of the Jet Propulsion Laboratory in 2003 [Dubovitsky, 2004]. The original model was written in MathCad, but was transferred to Matlab for use in this research.

The star-count model consists of four major steps, shown in Figure 4-24. First, the original list of candidate stars is read in, and stars are checked for eligibility. A star is not eligible for observations if it is part of a binary system with the stars too close together. Additionally, the TPF-I instrument has a specific sky-coverage, in terms of

ecliptic latitude. Therefore, a star that is outside of the latitude band covered by the instrument is not eligible for observation. Once the eligible stars are determined, observable stars are identified. If the instrument has the resolution capability to examine the habitable zone around an eligible star, that star is considered observable.

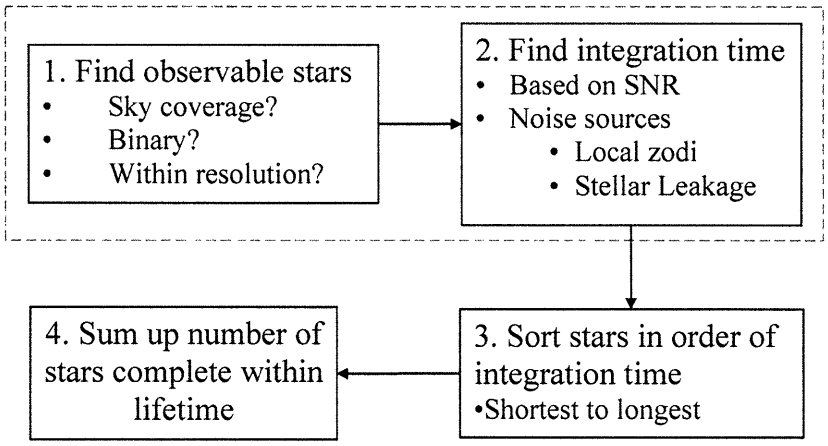


Figure 4-24: Four major steps of the star-count model. Only the steps within the red-dashed box are used if the model is used for expected productivity analysis.

The second major step in the star count model is finding the integration time for each star. This is by far the most complicated step in the process. Determining the required integration time is based on determining the signal and noise sources coming into the instrument. The power in photons incident from the planet, per second per square meter, is based on the assumed temperature of the planet, the radius of the planet, the distance to the star, and the minimum and maximum wavelengths under consideration. The total number of photons per second from the planet can then be calculated from the power per second per square meter, the total collecting area of the instrument, and a throughput factor for the instrument that accounts for the modulation efficiency, the beam combiner efficiency, the optics throughput, and the detector response.

The total noise into the system is calculated using two major factors - the local zodi and the stellar leakage. The number of photons per second per square meter from

the local zodi is calculated using a parametric model that includes the ecliptic latitude, the effective temperature of the dust, and the diameter of the apertures. The total number of photons per second received at the detector is then calculated using the number of photons per second per square meter, the total collecting area of all apertures, the same efficiency factor used for the planet signal calculation, and an additional throughput factor that is applied to incoherent signals. The second major noise source is stellar leakage. The stellar leakage is calculated from the luminosity of the star, the temperature of the star, the distance to the star, a factor based on the configuration of the architecture, and the length of the baseline. The total number of photons per second received at the detector from the stellar leakage is calculated using the same throughput values as the local zodi photon calculation.

Once the photon count per second for each signal and noise source is known, the signal to noise ratio acquired in a single second of operation can be calculated. The time required to achieve the necessary signal to noise ratio can then be calculated. This is shown in the following equations:

$$SNR_{1\text{sec}} = \eta \frac{S_{planet}}{\sqrt{S_{LocalZodi} + S_{Leakage}}}$$
$$T_{req} = \left(\frac{SNR_{req}}{SNR_{1\text{sec}}} \right)^2 \qquad (4\text{-}7)$$

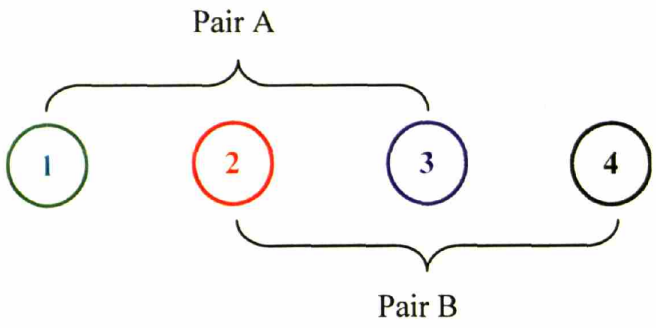
In the above equations, η is an efficiency factor based on the number of ports in the detector, S_{planet}, $S_{LocalZodi}$, and $S_{Leakage}$ are the total number of photons per second from the planet, the local zodi, and stellar leakage respectively, T_{req} is the total integration time required, SNR_{1sec} is the signal to noise ratio acquired in a single second of integration, and SNR_{req} is the required signal to noise ratio. The integration time required for either the detection or spectroscopy phase of the mission can be determined by adjusting the required signal to noise ratio.

As the length of the baseline increases, the stellar leakage also increases. This leads to an increase in the integration time. Therefore, it is more efficient, in terms of integration time, to have shorter baselines. If a baseline gets too short however, the

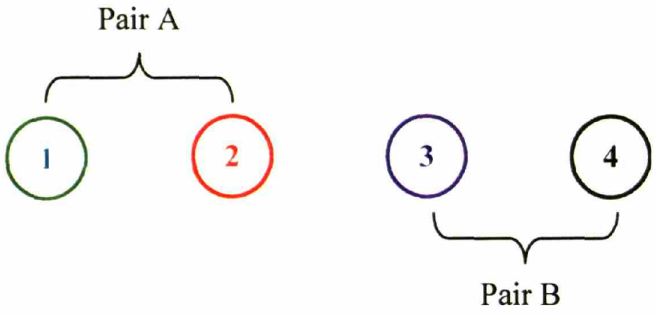
instrument will no longer have the resolution required to complete the observation. Therefore, for formation flown interferometers with variable baselines, the minimum baseline length required to achieve the necessary resolution for each star is calculated. If this length is less than or equal to the minimum allowable length of the baseline, set due to concern over collisions, the baseline length is set at the minimum allowable length. The maximum baseline length is set by stray-light concerns. If the baseline length required for the proper resolution is between the minimum and maximum allowable baseline lengths, the baseline length is set to the length required for the resolution. If the baseline length needed to achieve the proper resolution is larger than the maximum allowable length set by stray-light concerns, the star is not observable.

The final restriction on integration time deals with the time the star is visible to the instrument. The amount of time the star is visible depends on the ecliptic latitude of the star and the sky coverage of the instrument. The integration time plus any associated overhead time, based on the observational efficiency, must be less than or equal to the time the instrument can view the star. This constraint often has a large impact on the number of stars that can be observed by a particular architectural design.

One of the major TPF-I architectures has multiple possible observation modes, which means that the above process of determining integration times needs to be completed multiple times. The *Linear Dual Chopped Bracewell (DCB)* architecture has two separate modes – high resolution and low resolution. These modes are shown in Figure 4-25. For each star, the integration time required in each mode is calculated. The minimum of the two integration times is then used as the required integration time for that star.



a. High resolution mode



b. Low resolution mode

Figure 4-25: High versus low resolution modes for the *Linear DCB*

If the star-count model discussed here is used as the productivity model in an expected productivity analysis, the productivity metric is defined as the integration time per star. In these cases, only the first two steps shown in Figure 4-24 are used. If the star-count model is used without consideration of failures, the total number of observations that a particular instrument can complete in a given lifetime can be calculated. For the detection phase of the mission, the stars are sorted in order from shortest to longest integration times. The running sum of the integration times can then be used to calculate the number of observations that can be completed in the given lifetime.

For the spectroscopy phase of the mission, the calculation of the number of observations that can be completed is slightly more complicated. First, it is important to

ensure that spectroscopy observations are only done on stars for which observations were completed in the detection phase of the mission. It is also important to account for the fact that spectroscopy observations will only be possible for stars in which a planet was actually detected. In other words, spectroscopy is not possible if the detection phase observation was completed for a particular star, but no planet was found. However, there is no way of knowing ahead of time what the distribution of planets will be. If all the near-by stars have planets, the number of spectroscopy observations will be higher than if only the farther away stars have planets. To account for this, the total amount of time allowed for spectroscopy observations is first calculated as the lifetime of the spectroscopy phase of the mission divided by η_{Earth}, defined as the expected percentage of stars that have terrestrial sized planets within the habitable zone. The number of spectroscopy observations that can be completed within this extended time is then calculated using a running sum of the integration times. The expected number of spectroscopy observations is then calculated as this extended number of observations multiplied by η_{Earth}. The resulting expected number of spectroscopy observations then accounts for the spread of integration times possible, depending on which stars actually have detected planets in their habitable zone. [Dubovitsky, 2004]

4.4 TPF-I as a Case-study for Expected Productivity Analysis

TPF-I is a very complex and expensive mission in the very early design phases. While the timeline is still somewhat uncertain, launch is currently scheduled for 2019. With the launch date still over a decade away, major pre-formulation system architecture and spacecraft design decisions are still being made. These major decisions include the number of spacecraft, the type of beam combining, and the geometry of the array. It is at this early phase of a mission that introducing risk analysis into the trade process can have a major impact. TPF-I, therefore, makes a particularly good case-study for this research, since the results of any analysis can be used in design decision trade-studies, and can therefore affect the actual design of the mission.

It is well-accepted that analysis work done in the conceptual phases of a mission can have a very large impact on the overall outcome of the mission. Since cost, risk, and performance are commonly used as the three most important measures of effectiveness in trade-studies, it would stand to reason that cost, risk, and performance analyses should be used as factors when completing trade-studies in the conceptual design phases of a mission. While cost and performance are usually quantitatively analyzed and compared during these early phases, risk is most often analyzed in a qualitative way, if it is analyzed at all. This is due to the common misconception that a quantitative risk analysis can not be completed on a design that is in the conceptual stages, since every detail of the design must be known before the risk can be calculated. This research works to disprove that misconception by showing that a relative risk analysis can be done on any design that has a productivity model built, no matter how detailed the productivity model is. It was therefore important to use a mission that is in the conceptual design phase, such as TPF-I, as the case-study for this research, both to have as large an impact as possible on the design, and to prove that risk analyses can be completed, and be effective, when done early in the design phases of a mission.

While the reasons discussed above explain why the mission used as a case-study for this research should be in the early conceptual design phases, there are also several reasons why TPF-I makes one of the best conceptual design missions to use in this research. TPF-I is a formation flown interferometer, with five separate spacecraft. The multiple, individual spacecraft aspect of the mission lends itself to a set of obvious degraded states. Whether or not a particular architecture can function without a single spacecraft in the array, in addition to what is required to improve the chances of still having a functioning system if a single spacecraft were to fail, are very interesting risk-based analysis questions.

The interferometry aspect of TPF-I means that the mission is a perfect example of a mission with a path-dependant productivity function. The time to observe a given star depends not only on the functioning state of the instrument, but also on the stellar characteristics of that particular star. Additionally, the star-count model discussed in the previous section was used to calculate the integration time required for each star, for both

the nominal and degraded states of the instrument. This model is quite complicated and can take several minutes to calculate the integration time required for a single star. Therefore, running a Monte Carlo simulation using this productivity function could take an exceptionally large amount of time, possibly to the point of being prohibitive.

The final reason why TPF-I makes an excellent case-study for this research is that the expected productivity-based risk analysis results fill a gap in the current TPF-I set of analyses. For this mission, the number of stars observed is used as the major metric in architecture decisions. Prior to this work, all estimates of the star-counts did not take into account the possibility of any failures. Additionally, one of the major areas which the design team is working towards is reducing the perception, by both management and the public, that TPF-I will be a very risky mission. Completing a quantitative risk analysis that accounts for a conservative list of failure modes could help to reduce this perceived mission risk.

Chapter 5

CASE STUDY 1 - TPF-I ARCHITECTURAL TRADE STUDY FOR GRACEFUL DEGRADATION

5.1 Motivation

NASA needs to decide on a single architecture for the TPF-I mission to use as a baseline design. This baseline design will be used to study the expected performance and design issues of TPF-I. Additionally, the performance, cost, and risk of variations off this design can be compared to the equivalent parameters from the baseline design to determine the value of these variations. This mission is also known to require a very large amount of technology development and design work, forcing a need to begin working on a design as soon as possible in order to meet the proposed 2019 launch. Therefore, in December, 2004, NASA performed a down-select to a single architectural design for the TPF-I mission. In order to make a rational decision between different architectural options, these options needed to be quantitatively scored and compared against one another. This process of comparing the architectures was called the architecture trade study. The architectures under consideration in this study were the *Linear Dual-chopped Bracewell* (*DCB*), the *X-array*, the *Diamond DCB*, the *Z-array,* the *Triangle*, and the *Linear 3* [Lay et al., 2005].

Each of the architectures under consideration requires at least three separate spacecraft that need to be controlled to the centimeter level and need to function for at least five years. Additionally, this mission is assumed to be in the billion-dollar range in terms of cost. Given the extreme cost and the political ramifications of a failed mission,

along with the complexity of all of the designs and the probability of losing at least one spacecraft in five years, one of the characteristics that was listed as a discriminator between the architectures was how gracefully it is able to degrade. Graceful degradation implies that a single major failure will not result in a complete loss of the mission. The most obvious example of a single major failure is the loss of a single spacecraft. Therefore, the problem of examining how each of the architectures behaves after the loss of a single spacecraft was an important characteristic to examine in order to complete the architectural trade study for the down-select.

In order to determine the level of graceful degradation for a given architecture the degraded states for that architecture need to first be identified. The degraded states for any architecture are the states of the system in which there is still some level of functionality, but the system is no longer in the nominal state due to a failure. It should be noted that degraded states do not need to be as productive as the nominal states. In other words, a degraded state may have very little productivity and may not meet the requirements of the full, or even minimum, mission. The first goal of this study was to determine if any productivity at all would be possible in these degraded states, and if so to capture the basic characteristics of these states. Performance analyses were then completed for each degraded and nominal state. This information was then used to calculate the overall expected productivity of each of the architectures. If a degraded state from one of the architectures was significantly more productive than a degraded state from a different architecture than this difference was captured in the expected productivity. The expected productivity was then used as a quantitative value to compare the graceful degradation of each of the architectures for the architectural trade study. This chapter will first discuss the process of how each of the architectures was analyzed. The next section will discuss the basics of each architectural design, followed by a summary of how each of the architectures degrades. The results of the study will then be presented. Finally, some conclusions and summaries will be drawn.

5.2 Productivity in Degraded States

The first step in identifying the degraded states of any given architecture, in the event of the loss of a single spacecraft, was to identify the rules for determining when a system can still function. These rules were derived from the basic principles of interferometry. See Section 4.2 for a discussion on these basic principles. While it may be possible after some failures to do ancillary science that does not require interferometry, this was not considered a functioning state for the purposes of this study. For a given state to be considered a partially functional state, the following two criteria were required to be met:

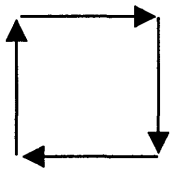
1. *Balanced path-lengths from at least three spacecraft capable of collecting light to a combining bench.*

2. *Zeroed-out input beam phases to the combiner.*

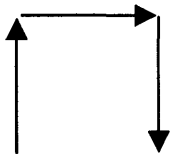
It should be noted that while the rule used for this study was that three spacecraft must be capable of collecting light, it is possible to do very basic interferometry with only two collecting spacecraft. With two beams it is not possible to achieve chopping between sources, however. The process of chopping changes from one set of beams to another in order to greatly reduce the level of systematic noise in the data. Given the TPF-I requirements for very low noise levels, it was decided that chopping will be required for the type of science that TPF-I is doing. Therefore, in this study at least three functioning starlight beams were required to be combined to be considered a functional state. While states capable of combining only two starlight beams were considered zero-productivity states, these states were recorded in the study, in case chopping is not considered a necessity in the future.

The path-lengths from each source to the combiner need to be equalized in order to achieve interferometry. The beam paths can go directly to the combiner or, if the system is designed to support it, the beams can go through other spacecraft before reaching the combiner or through a delay line to equal out the path lengths. The phases of the separate beams also need to be zeroed out in order for interferometry to work. This is explained further in Figure 5-1. The arrows in Figure 5-1 represent the beams of

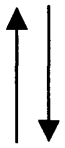
different sources or collectors. The length of the arrow represents the amplitude of the beam while the direction represents the phase. Figure 5-1a shows the beams for a four-collector interferometer. Note that the end of the last, or fourth, arrow is in the same location as the beginning of the first arrow. This is called zeroing out the beams. Figure 5-1b shows this same architectural set-up but with a single spacecraft missing. Note that the beams no longer meet up, or zero out. Using only the first and third beams in this configuration would zero out the beams as shown in Figure 5-1c. If the phases, or directions of the arrows, were variable, all three beams could be zeroed out, as seen in Figure 5-1d. This implies that a four-collector system with fixed phases would be reduced to a two-collector system with the failure of a single spacecraft. But it could use all three collectors if the system was designed to allow for variable phases, and if the path lengths from the three sources to the combiner are still equal.



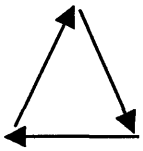
a. Initial Phase Diagram



b. If one spacecraft fails, the phases no longer sum to zero



c. Can still zero out the phases using only 2 spacecraft



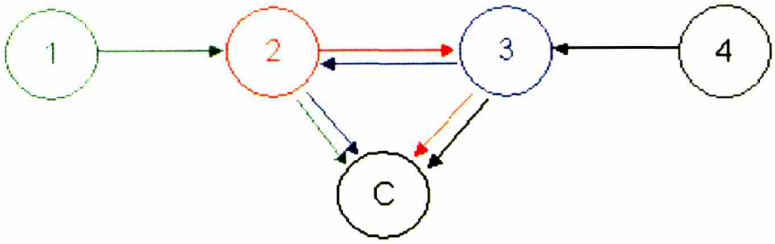
d. To use 3 spacecraft, you need to be able to vary the phases

Figure 5-1: Phase diagrams to show the concept of zeroing out phases.

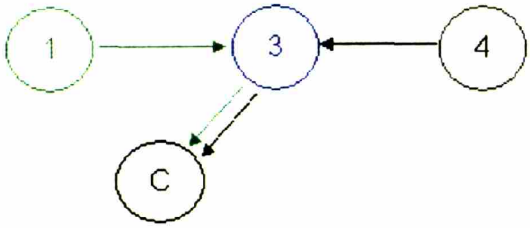
For each of the architectures under consideration the unmodified design, in terms of beam paths and phases, was examined to see if the degraded system, without any one given spacecraft, could meet the two criteria specified above. If the criteria were met, the type of the degraded system was noted. The number of collecting elements and the geometry of the spacecraft define the type of system. An example of a type of system is a two-collector system in which the collectors are placed in a line relative to one another, called a *Linear 2* in this study. After the degraded states of the unmodified design were examined, different options were identified which change the design in order to attempt to increase the likelihood of graceful degradation.

The unmodified design for each of the architectures was assumed to have fixed phases. Adding the ability to vary phases after launch was the first change examined. Adding the ability to vary the angles of the input and output beams to and from each spacecraft, such that the geometry of the spacecraft relative to one another could vary from the nominal design, was the second change considered. Finally, for each of the architectures a single additional major change was identified that would make a large impact on the degradation of the architecture. This change varied from architecture to architecture and included making spacecraft identical to one another, adding extra beam routing paths, or adding a delay line. In some cases, if either variable phases or variable angles in and out of the spacecraft had zero impact on the degraded state analysis, two other changes that are specific to that architecture were examined. This analysis resulted in anywhere from four (2^2) to eight (2^3) designs per architecture.

Each design is defined as a combination of hardwired (non-variable) or variable phases, fixed or variable beam angles, and making or not making another one or two major changes to the design. The functionality of each design given a failure of each individual spacecraft was examined. The final result of this analysis for each of the architectures is a table similar to the example shown in Table 5-1, along with figures similar to the example shown in Figure 5-2.



a.
Nominal



b.
Degraded state: Linear 2

Figure 5-2: Degraded state diagram example

Figure 5-2a shows the nominal number and geometry of spacecraft, and the beam-routing paths, for an example architecture. Each circle represents a spacecraft and is labeled by a letter or number. The beam paths are color coded in order to keep track of which beam comes from which spacecraft. The rows of the table that accompany these diagrams, in this case Table 5-1, correspond to the particular spacecraft that is considered failed. The rows are labeled in the same manner as the spacecraft in the diagrams. The columns of the table correspond to the different designs examined. Each entry in the table is the type of system that would remain if that particular spacecraft (row) failed in that particular design (column). In the same manner that Figure 5-2a shows the nominal spacecraft geometry and beam paths, the degraded state diagrams, in this case Figure 5-2b shows the spacecraft geometry and beam paths for each type of degraded system found in the table (Table 5-1).

Table 5-1: Degraded state table example

	Angles in/out set, Hardwired phases, All different	Angles in/out set, Hardwired phases, 1=2,3=4	Angles in/out set, Variable phases, All different	Angles in/out set, Variable phases, 1=2,3=4	Angles in/out variable, Hardwired phases, All different	Angles in/out variable, Hardwired phases, 1=2,3=4	Angles in/out variable, Variable phases, All different	Angles in/out variable, Variable phases, 1=2,3=4
1	Linear 2	Linear 2	Linear 3	Linear 3	Linear 2	Linear 2	Linear or Triangular 3	Linear or Triangular 3
2	Linear 2	Linear 2	Linear 2	Linear 3	Linear 2	Linear 2	Linear 2	Linear or Triangular 3
3	Linear 2	Linear 2	Linear 2	Linear 3	Linear 2	Linear 2	Linear 2	Linear or Triangular 3
4	Linear 2	Linear 2	Linear 3	Linear 3	Linear 2	Linear 2	Linear or Triangular 3	Linear or Triangular 3
C	X	X	X	X	X	X	X	X

It should be noted that the degraded state diagrams that are associated with each of the architectures are examples of the different types of degraded state systems. If the same type of system would remain if two different spacecraft were to fail, the system was only drawn in diagram form for one of the two scenarios. An example of this can be seen in Figure 5-2. In this example a *Linear 2* system is shown as an example of a degraded state. Table 5-1 corresponds to this example and shows that a *Linear 2* system is left if several different spacecraft fail for several different designs. The diagram corresponds to the failure of spacecraft two. This is because all *Linear 2* systems would be similar and are therefore not drawn individually. If spacecraft three failed instead of spacecraft two the diagram would be identical to that shown, except in mirror image and with spacecraft three replaced by spacecraft two. Note also that spacecrafts two and three both have output beams in the same geometry as spacecrafts one and four, respectively. Therefore, if spacecraft one were to fail instead of spacecraft two, the same *Linear 2* diagram would be applicable but with spacecraft two replacing spacecraft one, and the same is true for

three and four. Since the geometry and beam-routing paths are identical in all four cases, the *Linear 2* system is only drawn once as an example.

The examples shown in Figure 5-2 and Table 5-1 are for a *Linear Dual-chopped Bracewell* (*DCB*) system. This example will be discussed and explained further in the following section, followed by the discussion, tables, and diagrams for each of the five other architectures examined.

5.2.1 Linear DCB

The nominal *Linear Dual-Chopped Bracewell* (*DCB*) design is shown in Figure 5-3. This design requires four collecting spacecraft, labeled 1-4, and a separate combining spacecraft, labeled C. The beams from the outer collectors are routed through the inner collectors to the combiner. The beams from the inner collectors are routed through the other inner collector to the combiner. The architecture is symmetrical, such that spacecrafts one and two are mirror images of spacecrafts three and four, respectively.

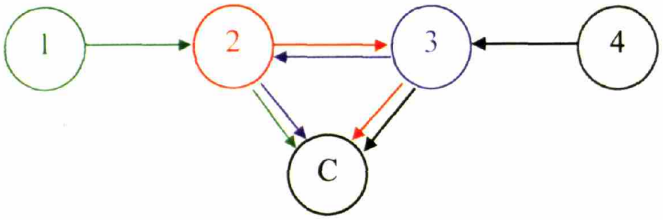


Figure 5-3: Nominal configuration for the *Dual-Chopped Bracewell* architecture.

The first thing of note about the *Linear DCB* architecture is that if the combining spacecraft were to fail the mission would be over. In this sense, the combiner is the weakest link of this design. If spacecraft one were to fail the beams from spacecraft two, three, and four could follow the same paths as in the nominal design and the path-lengths would be equal. The same is true if spacecraft four failed. In the unmodified design, without variable phases, only two of these collectors would be useful since that is the only way to zero-out the phases, as discussed above. If phases are allowed to vary, the

system could reach a three spacecraft linear system. If spacecraft two were to fail however, then spacecraft three would have no method of equalizing its path length with those from spacecraft one and four, and only a two-collector system would be possible. If the angles in and out of the spacecraft were variable and a three-collector system was possible, a triangular geometry could also be used. Finally, the major design change examined for this architecture was making spacecrafts one and four identical to spacecrafts two and three respectively. This removes the two-collector system restraint if spacecraft two or three fails. The summary table of all possible degraded states for the *Linear DCB* architecture is shown in Table 5-2 and the corresponding degraded state diagrams are shown in Figure 5-4.

Table 5-2 : Degraded states for the *Linear DCB* architecture.

	Angles in/out set, Hardwired phases, All different	Angles in/out set, Hardwired phases, 1=2,3=4	Angles in/out set, Variable phases, All different	Angles in/out set, Variable phases, 1=2,3=4	Angles in/out variable, Hardwired phases, All different	Angles in/out variable, Hardwired phases, 1=2,3=4	Angles in/out variable, Variable phases, All different	Angles in/out variable, Variable phases, 1=2,3=4
1	Linear 2	Linear 2	Linear 3	Linear 3	Linear 2	Linear 2	Linear or Triangular 3	Linear or Triangular 3
2	Linear 2	Linear 2	Linear 2	Linear 3	Linear 2	Linear 2	Linear 2	Linear or Triangular 3
3	Linear 2	Linear 2	Linear 2	Linear 3	Linear 2	Linear 2	Linear 2	Linear or Triangular 3
4	Linear 2	Linear 2	Linear 3	Linear 3	Linear 2	Linear 2	Linear or Triangular 3	Linear or Triangular 3
C	X	X	X	X	X	X	X	X

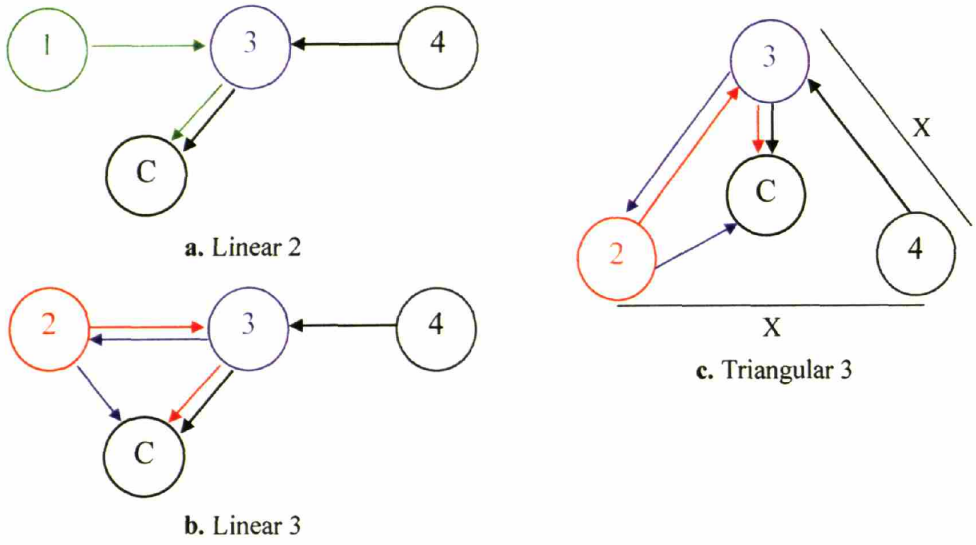


Figure 5-4 : Degraded states for the *Linear DCB* architecture.

5.2.2 X-array

The nominal *X-array* design is shown in Figure 5-5. This design requires four collecting spacecraft, labeled 1-4, and a separate combining spacecraft, labeled C. The four collecting spacecraft are identical. The advantage to this design is that the 3-to-1 aspect ratio of the rectangular geometry allows for a relatively long resolution baseline while keeping a relatively short nulling baseline. The resolution baseline is the distance between the spacecraft on the long side of the rectangle. A long resolution baseline leads to increased capability to resolve the signals from multiple planets. The nulling baseline is the distance between the spacecraft on the short side of the rectangle. A short nulling baseline leads to increased capability to reject the light from the target star. While many designs have a single baseline length, which needs to be set at a compromise value since longer is better for resolution and shorter is better for nulling, the *X-array* design has separate baselines which leads to more optimal lengths for each individual function [Lawson & Dooley, 2005].

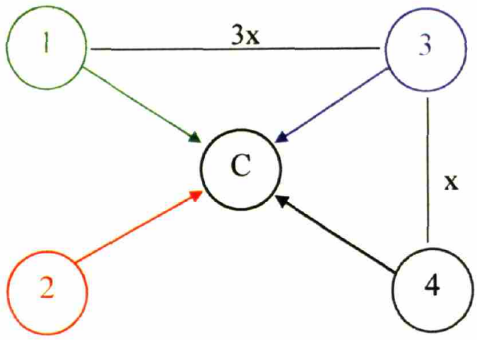
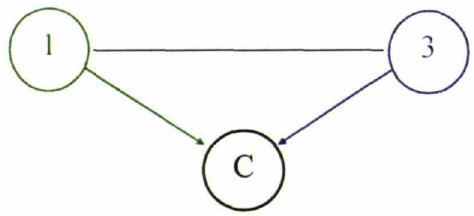


Figure 5-5 : Nominal configuration for the *X-array* architecture.

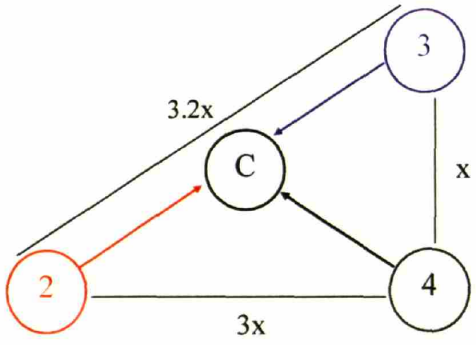
The *X-array* design degrades very gracefully, with many options for degraded states. As with the *Linear DCB* design, the combiner is the weak link in this design since if it fails, the mission is lost. Also as with all other four-collector architectures, if a single collector fails, but the unmodified design without variable phases is used, the system is forced into a two-collector system due to the phases. If the phases are variable however, several three-collector options are possible. Since all four collectors are identical the system acts the same no matter which collecting spacecraft is assumed failed. If the beam angles in and out of the spacecraft are not variable, the system degrades to a three-collector system with three different baselines, called *3 Single*. If the beam angles in and out of the spacecraft are somewhat variable, the system can degrade to a 3-collector system with two identical baselines and one unique baseline, called *2 Same*. The major design change examined for the *X-array* was to allow the angle of the beams into the combiner to vary by as much as 70 degrees. In this case the system can degrade to a three-collector system with three identical baselines, called *3 Same*. The summary table of all possible degraded states for the *X-array* architecture is shown in Table 5-3 and the corresponding degraded state diagrams are shown in Figure 5-6. It should be noted that there is no need for extra beam routing or other major changes with the *X-array* design. This system degrades quite gracefully with relatively minor changes (variable phases and variable angles into the combiner).

Table 5-3 : Degraded states for the *X-array* architecture.

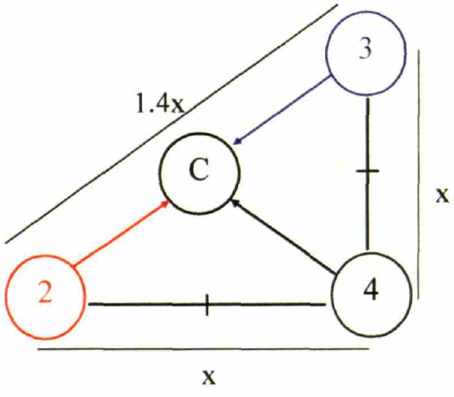
	Angles in/out set, Hardwired phases	Angles in/out set, Variable phases	Angles in/out variable, Hardwired phases	Angles in/out variable, Variable phases	Angles in/out extra variable, Variable phases
1	Linear 2	3 Single	Linear 2	2 Same	3 Same
2	Linear 2	3 Single	Linear 2	2 Same	3 Same
3	Linear 2	3 Single	Linear 2	2 Same	3 Same
4	Linear 2	3 Single	Linear 2	2 Same	3 Same
C	X	X	X	X	X



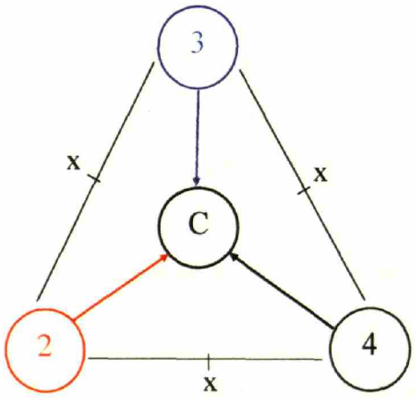
a. Linear 2



b. 3 Single



c. 2 Same



d. 3 Same

Figure 5-6 : Degraded states for the *X-array* architecture.

5.2.3 Triangle

The nominal *Triangle* architecture is shown in Figure 5-7. This architecture consists of only three spacecraft. One of these spacecraft, in this case spacecraft number three, functions as both a collecting spacecraft and a combining spacecraft.

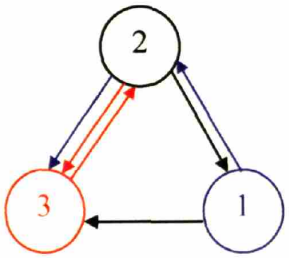
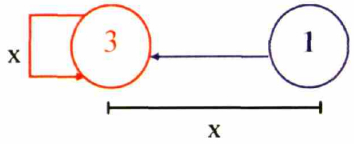


Figure 5-7: Nominal configuration for the *Triangle (TTN)* architecture.

The *Triangle* architecture degrades very ungracefully since there is no redundancy built into the system. With the unmodified design the mission would be over with a single failure to any of the three spacecraft. This is true of the design with variable phases or with variable beam angles into and out of the spacecraft. The only way to produce a degraded state that is still functional is to add an extremely long delay line to the combining spacecraft, equal to the distance between the spacecraft. This addition would introduce a significant amount of extra complexity and weight and almost certainly not be considered. The only way to ensure some functionality in the case of any single failure for this system is to both add a very long delay line to the combining spacecraft, and to make spacecraft two identical to spacecraft three. The summary table and corresponding diagrams for the *Triangle* architecture can be seen in Table 5-4 and Figure 5-8, respectively.

Table 5-4: Degraded states for the *Triangle* architecture.

	No Long Delay Line All different	No Long Delay Line 2=3	Long Delay Line All different	Long Delay Line 2=3
1	X	X	Static Linear 2	Static Linear 2
2	X	X	Static Linear 2	Static Linear 2
3	X	X	X	Static Linear 2



Static Linear 2

Figure 5-8 : Degraded state for the *Triangle* architecture.

5.2.4 Diamond DCB

The nominal configuration for the *Diamond DCB* architecture is shown in Figure 5-9. The *Diamond DCB* design has four collecting spacecraft and no separate combining spacecraft. Instead, the combining is done on one of the existing collecting spacecraft: spacecraft four.

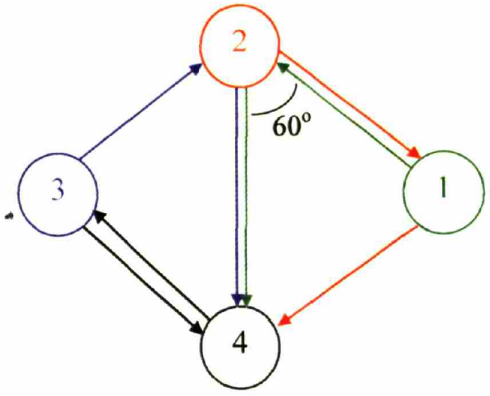


Figure 5-9 : Nominal configuration for the *Diamond DCB* architecture.

In the *Diamond DCB* design there is no added bonus to varying the angles into or out of any of the spacecraft. Therefore, in addition to adding variable phases to the design, two other major changes to the design were examined - adding extra beam routing, and adding combining ability to spacecraft two. The extra beam routing paths that would be required are shown in Figure 5-10 by the dashed arrows. Note that not all of these extra beam paths would need to be implemented. If only a subset of these beam paths were added, only a subset of the degraded states that result from these paths would be available.

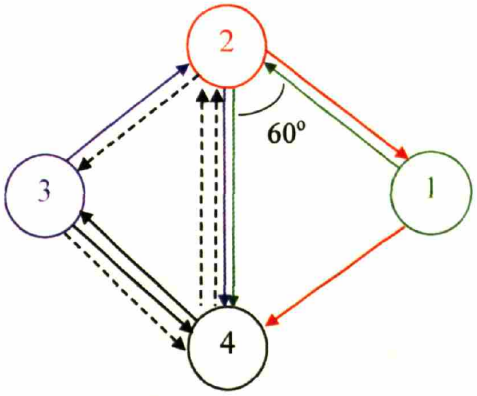
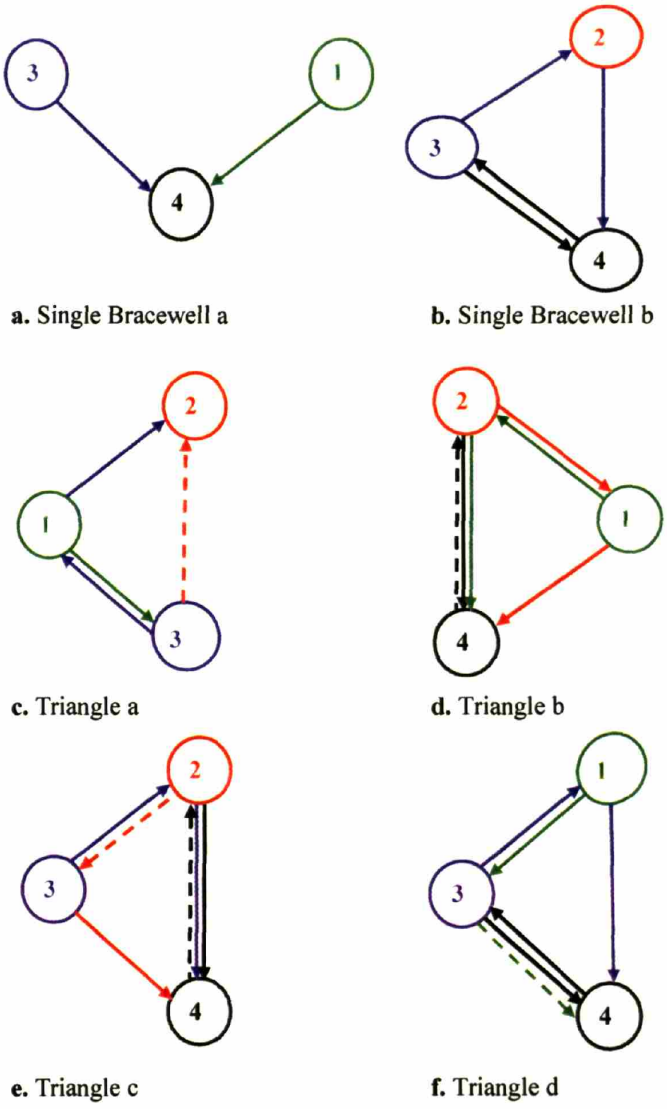


Figure 5-10 : Extra beam routing path options for the *Diamond DCB* architecture. The dashed arrows show the extra beam paths.

As with the architectures with separate combiner spacecraft, in the *Diamond DCB* design the combiner, in this case spacecraft number four, is the weak link since if it fails the mission is lost. This effect is reversed however if spacecraft two is given combining capability. Also, as with all other four-collector architectures, if a single collector fails in the *Diamond DCB* design without variable phases, the system is forced into a two-collector system. Due to phasing limitations, beams from spacecrafts two and three cannot be combined together in a single Bracewell format. Therefore, if spacecraft one fails and phases can not be varied, a different version of the single Bracewell is required. With variable phases and extra beam routing added to the design, the system can degrade to a three-collector, *Triangle* design. It is of interest to note that there is no advantage to having variable phases with this architecture unless extra beam routing paths are also added, since no beam routing path could achieve a three-collector system without adding extra beam paths to the current design. The summary table of the degraded state possibilities for the *Diamond DCB* architecture and the corresponding diagrams are shown in Table 5-5 and Figure 5-11. Since the *Triangle* degraded states require different elements of extra beam routing, all versions of this design are shown separately.

Table 5-5 : Degraded states for the *Diamond DCB* architecture.

	Hardwired phases, No extra beam routing, 2 not combiner	Hardwired phases, Extra beam routing, 2 not combiner	Hardwired phases, No extra beam routing, 2 combiner	Hardwired phases, Extra beam routing, 2 combiner	Variable phases, No extra beam routing, 2 not combiner	Variable phases, Extra beam routing, 2 not combiner	Variable phases, No extra beam routing, 2 combiner	Variable phases, Extra beam routing, 2 combiner
1	Single Bracewell b	Single Bracewell b	Single Bracewell a	Single Bracewell a	Single Bracewell a	Triangle c	Single Bracewell a	Triangle c
2	Single Bracewell a	Single Bracewell a	Single Bracewell a	Single Bracewell a	Single Bracewell a	Triangle d	Single Bracewell a	Triangle d
3	Single Bracewell a	Single Bracewell a	Single Bracewell a	Single Bracewell a	Single Bracewell a	Triangle b	Single Bracewell a	Triangle b
4	X	X	Single Bracewell a	Single Bracewell a	X	X	Single Bracewell a	Triangle a



a. Single Bracewell a

b. Single Bracewell b

c. Triangle a

d. Triangle b

e. Triangle c

f. Triangle d

Figure 5-11 : Degraded states for the *Diamond DCB* architecture.

5.2.5 Z-array

The nominal configuration for the *Z-array* architecture is shown in Figure 5-12. The *Z-array* is very similar to the *X-array* architecture. The advantage of the 3-to-1 aspect ratio of the rectangular geometry, allowing for a relatively long resolution baseline while keeping a relatively short nulling baseline, is true for both architectures. The difference between the two architectures is that in the *X-array* there is a separate spacecraft for combining the light, and in the *Z-array* the combining is done on one of the collecting spacecraft. In this architecture all beams are combined and modulated in

spacecraft one. Note that the *Z-array* architecture is not symmetric. Spacecraft three is the only spacecraft with a simple beam routing design, with only a single output beam. Therefore, for this architecture, in addition to variable phases and variable beam angles, the major design change considered was to make spacecraft three a mirror image of spacecraft one. While this design change obviously makes spacecraft three more complex, it should be noted that this design change does reduce the number of different spacecraft designs required, which could save some money and effort. This modified design can be seen in Figure 5-13.

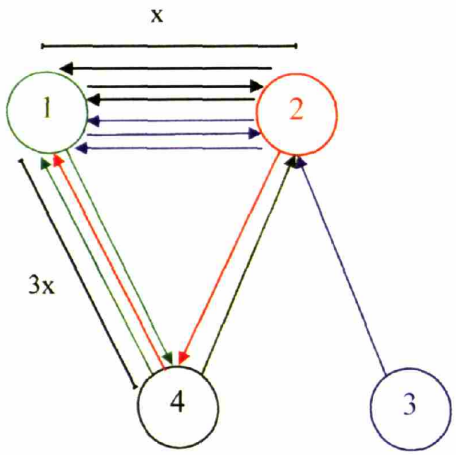


Figure 5-12 : Nominal configuration for the *Z-array* architecture.

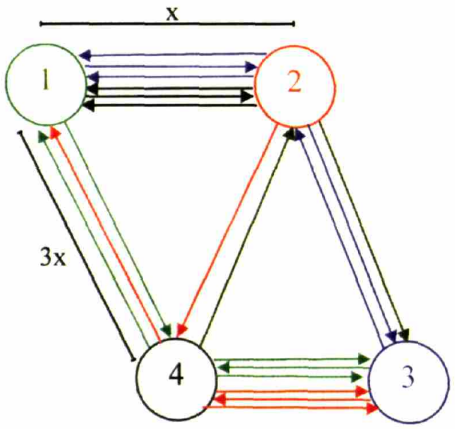


Figure 5-13 : Modified design for the *Z-array* architecture - spacecraft 3 is the mirror image of spacecraft 1.

With the *Z-array* architecture, all combining and modulating occurs in spacecraft one. Therefore, in the unmodified design, without spacecraft three mirroring spacecraft

one, if spacecraft one fails the entire mission fails. Additionally, the unmodified design for the *Z-array* architecture has the restriction that spacecraft three can only transfer its beam to spacecraft two. This essentially leads to the equivalent of a failure in spacecraft three if spacecraft two were to fail, since spacecraft three could no longer transfer its beam to the rest of the system. Since no interferometry would be possible with only the two spacecraft, if spacecraft two fails in the unmodified design, the entire mission fails. If the angles into and out of the spacecraft are allowed to vary then the output from spacecraft three could be varied to allow transfer of its beam to other spacecraft, taking away this restriction. The simplicity of the design for spacecraft three, with only a single output beam, also restricts the system to degrading to a two-collector system, even in the case of variable phases and angles. As with all other four-collector systems, it is not possible to degrade to a three-collector system without variable phases. The table of degraded states and corresponding figures for the *Z-array* architecture can be seen in Table 5-6 and Figure 5-14, respectively. While the fully modified design for the *Z-array* architecture degrades very gracefully, it is important to note that in this case the graceful degradation comes at the cost of a very complex nominal configuration, as shown in Figure 5-13.

Table 5-6: Degraded states for the *Z-array* architecture.

	Angles in/out set, Hardwired phases, All different	Angles in/out set, Hardwired phases, 3=mirror image of 1	Angles in/out set, Variable phases, All different	Angles in/out set, Variable phases, 3=mirror image of 1	Angles in/out variable, Hardwired phases, All different	Angles in/out variable, Hardwired phases, 3=mirror image of 1	Angles in/out variable, Variable phases, All different	Angles in/out variable, Variable phases, 3=mirror image of 1
1	X	Single Bracewell b	X	Triangle b	X	Single Bracewell b	X	Triangle b
2	X	Single Bracewell b	X	Single Bracewell b	Single Bracewell a	Single Bracewell b	Single Bracewell a	Triangle a or b
3	Single Bracewell a	Single Bracewell a	Triangle a	Triangle a	Single Bracewell a	Single Bracewell a	Triangle a	Triangle a
4	Single Bracewell a	Single Bracewell a	Single Bracewell a	Single Bracewell a	Single Bracewell a	Single Bracewell a	Single Bracewell a	Triangle a or b

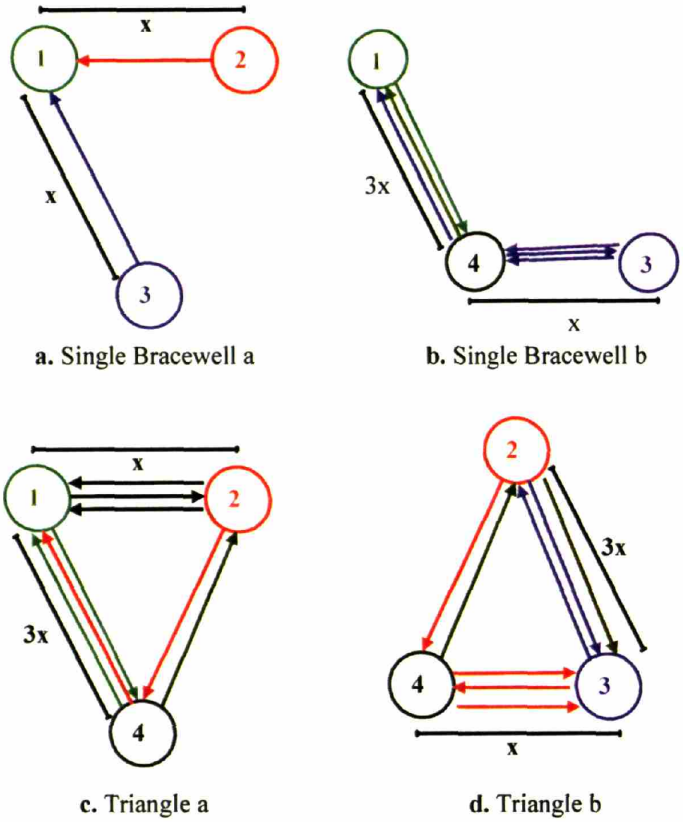


Figure 5-14 : Degraded states for the *Z-array* architecture.

5.2.6 Linear 3

The nominal configuration for the *Linear 3* architecture is shown in Figure 5-15. The *Linear 3* architecture is identical to the *Linear DCB* architecture, except the *Linear 3* architecture has only three collecting spacecraft in the nominal configuration. The *Linear 3* architecture is actually one of the degraded state architectures for the *Linear DCB*.

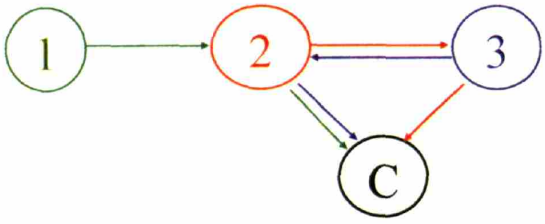
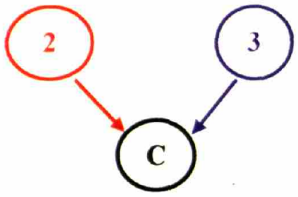


Figure 5-15: Nominal configuration for the *Linear 3* architecture.

The *Linear 3* architecture degrades very ungracefully, since there is no redundancy built into the system, assuming three collecting spacecraft are required. The unmodified design could degrade to a single Bracewell architecture if the single outer spacecraft is lost. This same two-collector system could be achieved if either spacecraft one or spacecraft two is lost, and spacecraft one is given the extra beam routing capability of spacecraft two. Additionally, this two-collector system could be achieved with any spacecraft failure, other than the combiner, if the angles out of the collectors are allowed to vary. The two-collector system was assumed to have zero productivity, since chopping was required. Therefore, under the current assumptions, the *Linear 3* architecture degrades very ungracefully. If, however, future studies find chopping is not required, this system could do very well in terms of graceful degradation. The summary table and corresponding diagrams for the *Linear 3* architecture can be seen in Table 5-7 and Figure 5-16, respectively.

Table 5-7: Degraded states for the *Linear 3* architecture.

	Angles in/out set, Hardwired phases, All different	Angles in/out set, Hardwired phases, 1=2	Angles in/out set, Variable phases, All different	Angles in/out set, Variable phases, 1=2	Angles in/out variable, Hardwired phases, All different	Angles in/out variable, Hardwired phases, 1=2	Angles in/out variable, Variable phases, All different	Angles in/out variable, Variable phases, 1=2
1	Single Bracewell	Single Bracewell	Single Bracewell	Single Bracewell	Single Bracewell	Single Bracewell	Single Bracewell	Single Bracewell
2	X	Single Bracewell	X	Single Bracewell	Single Bracewell	Single Bracewell	Single Bracewell	Single Bracewell
3	X	X	X	X	Single Bracewell	Single Bracewell	Single Bracewell	Single Bracewell
C	X	X	X	X	X	X	X	X



a. Single Bracewell

Figure 5-16: Degraded state for the *Linear 3* architecture.

5.3 Study Results

As discussed above, the architecture trade study completed by the TPF-I design team compared the performance, cost, and risk of all the previously discussed architecture options. While graceful degradation was considered an important parameter to include in the trade study, it was by no means the only consideration. Each of the architectures was judged in terms of a total of 27 different discriminators, including the ability to degrade gracefully. A given discriminator was quantified by giving a numerical score to each of the architectures in terms of one or more parameters.

To capture the needs of the TPF-I design team, the graceful degradation category was split into two separate parameters. The first parameter assumed a single spacecraft failure prior to the beginning of operations. No other failures throughout the lifetime of the mission were considered. This parameter was designed to reward an inherent robustness to failures. Architectures are more desirable if it is possible to have some productivity in the event of a major failure. The level of productivity will vary depending on which spacecraft failed, but this was accounted for by determining the productivity of the system with a failure of each individual spacecraft, and finding the average of all scenarios.

The second parameter used to quantify the ability of the different architectures to degrade gracefully was the total overall expected productivity. In this case, each spacecraft was assumed to have a 5% probability of failure prior to operations, in addition to a 5% probability of failure by the end of the mission lifetime. If a single spacecraft both collects and combines light these probabilities of failure were doubled,

since the spacecraft was assumed to be significantly more complicated than a spacecraft performing only one of these functions. This parameter took into account not only the productivity of the remaining system after a single spacecraft failed, but also the probability and timing of these failures. For this parameter, the EPRA modeling approach discussed in Chapter 3 was used to calculate the expected productivity.

For both parameters, expected productivity was measured by the total expected star-count in the detection phase of the mission. The star-count in the detection phase, without considering failures, was already taken into account in the architectural trade study. Since those architectures with higher productivity in their nominal states should not get double points for these higher nominal productivities, both of the graceful degradation parameters were normalized by the nominal star count levels. Therefore, the final parameters used to measure graceful degradation in the trade study were:

- The expected percentage of the nominal detection star-count assuming a single spacecraft failure, and

- The total expected percentage of the nominal detection star-count given a 5% probability of failure, for both pre-operations failures and failures throughout life, for each spacecraft with a single function.

In all cases the star-count model described in Chapter 4 was used to determine the productivity of all nominal and degraded states.

As mentioned above, none of the architectures considered could lose a single spacecraft and have any productivity in the remaining system, without adding variable phases to the design. Adding variable phases to the design is a significantly easier design change to make than adding variable beam angles in and out of the spacecraft. Additionally, comparing the other major design changes that were unique to each of the architectures was not appropriate in this trade study, since the complexity and difficulty of adding these design changes varies from one design change to another. Therefore, for the architectural trade study, all architectures were compared assuming original designs with variable phases, and no other design changes were considered.

The results of study are given below. Table 5-8 shows the expected percentage of the nominal detection star-count, assuming a single spacecraft failure. The specific degraded states that led to the productivity values given in Table 5-8 can be seen in the tables and degraded state diagrams associated with each of the architectures in Section 5.2.

In terms of this discriminator, the *X-array* architecture performs the most favorably, followed closely by the *Linear DCB* architecture. The main thing to note in Table 5-8 however is not the architectures that perform well, but the architectures that do not perform well. The *Triangle, Diamond DCB,* and *Linear 3* architectures would have zero productivity if any of the spacecraft in the architecture were to fail. This is a significant negative aspect of all three of these architectures.

Figure 5-17 shows the expected percentage of the nominal star-count for each of the architectures, assuming a 5% probability of failure, both by the beginning of operations and the end of life, for each single-function spacecraft. The performance of all architectures, in terms of this particular parameter, is relatively similar. This is due to the trade-off between probability of failure and impact. Architectures that initially have four spacecraft capable of collecting light can lose a single collecting spacecraft and still function, making the impact of a failure significantly less than for those architectures that nominally begin with only three collecting spacecraft. Since the probability of failure is on a per-spacecraft basis however, the architectures that nominally have four collecting spacecraft also have a higher probability of losing a spacecraft than those with only three collecting spacecraft. These two effects nearly cancel each other out. This result does not lessen the importance of the study. Prior to this work, many engineers on the design team conveyed opinions that architectures with fewer spacecraft were less risky due to the lower probability of failure. At the same time, other engineers viewed these same architectures as more risky due to the increased impact of a failure. The result that the productivity in degraded states for this case-study nearly balances out the additional probability of failure incurred with extra spacecraft, is both interesting and not necessarily intuitive. Without completing the study, and determining the productivity in

the degraded states, there would not have been a way to know which of the architectures performed better or worse in terms of this parameter.

When comparing the *X-array* to the *Z-array* or the *Linear 3* to the *Triangle* architecture, the architectures with a separate combining spacecraft (*X-array* and *Linear 3*) perform better in terms of overall expected productivity than those architectures with a dual-functioning spacecraft. This is partially because, from a probabilistic stand-point, having one extra spacecraft with a given failure rate is slightly better than having one less spacecraft, but with one of the spacecraft having twice the failure rate. This can be seen by comparing 0.95^2, or 0.9025, to 0.9. Note that the difference between these architectures will be due not only to this probabilistic difference, but also to the difference in productivity in degraded states, and the difference in productivity of the nominal state.

While only by a relatively small margin, the *X-array* and the *Linear-3* architectures do perform best in terms of the overall expected productivity. This makes sense, since the *Linear-3* architecture has the lowest probability of a failure occurring, and the *X-array* architecture has the best productivity in degraded states. The *Diamond* and *Z-array* architectures perform the worst in terms of this parameter. This is due to the fact that both architectures have four spacecraft capable of collecting light, leading to a higher probability of failure, but the *Diamond* architecture does not have a degraded state that has any productivity if a single spacecraft is lost, and the *Z-array* architecture has only a single productive degraded state.

Table 5-8: Normalized expected productivity results assuming a single spacecraft failure.

	Linear DCB	X-array	Triangle	Diamond	Z-array	Linear 3
Col. 1	41%	28%	0%	0%	0%	0%
Col. 2	0%	28%	0%	0%	0%	0%
Col. 3	0%	28%	0%	0%	34%	0%
Col. 4	41%	28%	N/A	0%	0%	N/A
Comb.	0%	0%	N/A	N/A	N/A	0%
Average	16%	22%	0%	0%	8%	0%

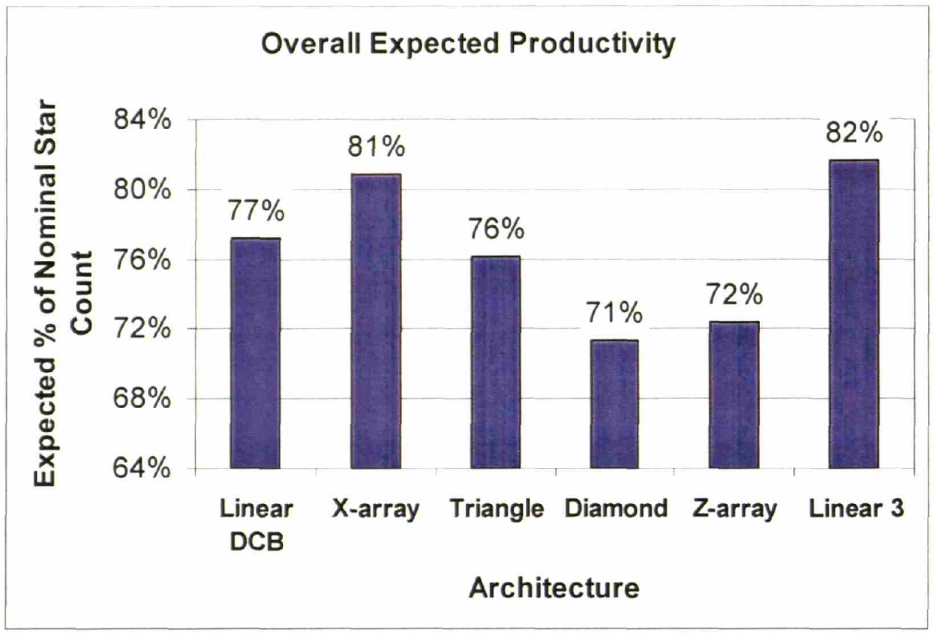


Figure 5-17: Overall expected productivity results assuming a 5% probability of failure per spacecraft both pre-operations and throughout life.

The results shown assume a 5% probability of failure, both before operations begin and by the end of life, for each spacecraft with a single function. The probabilities of failure for spacecraft that are required to both collect and combine light were doubled to 10%. The 5% value was based purely on engineering judgment. Therefore, a sensitivity study was carried out to examine how much the specific probability of failure chosen impacts the study results. The results of the sensitivity study can be seen in Figure 5-18, where the value on the x-axis corresponds to the probability of failure for a single-function spacecraft. The same probability of failure was used in all cases for both the pre-operations probability of failure and the probability of a failure occurring by the end of life. An exponential failure rate was assumed for failures that could occur throughout life. In all cases the failure rates were doubled for any spacecraft that is required to both collect and combine light.

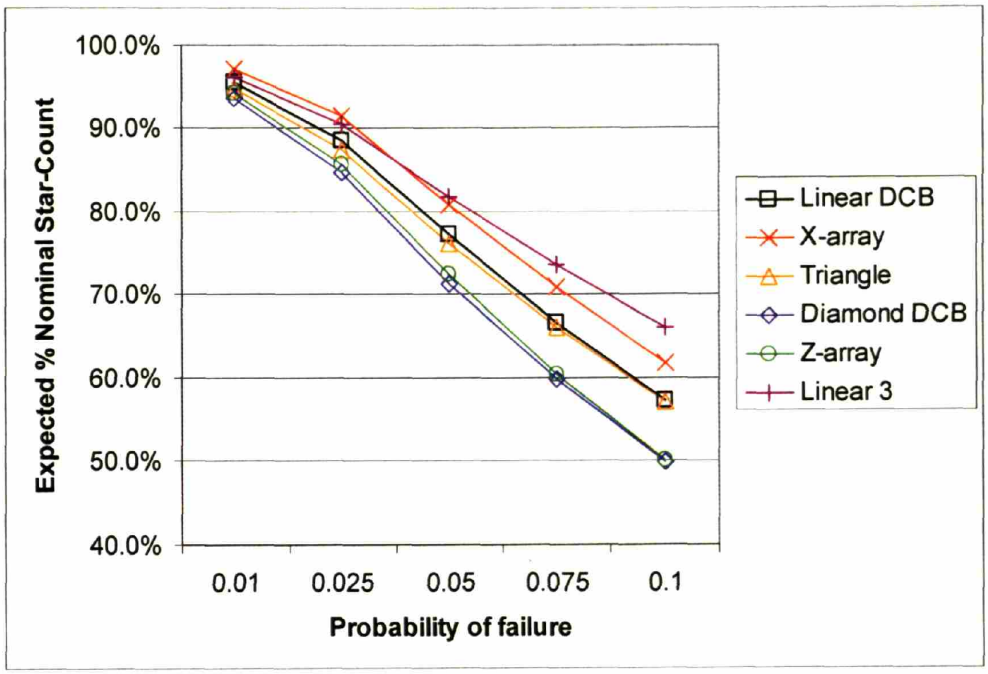


Figure 5-18: Sensitivity study of overall expected productivity results.

Figure 5-18 shows that the results of this study are not particularly sensitive to the value assigned to the probability of failure. In all cases the relative pattern between architectures remains reasonably consistent. The *Diamond* and *Z-array* architectures consistently perform worst, followed by the *Triangle* and *Linear DCB* architectures. The *X-array* and *Linear 3* architectures consistently perform better than the other four architectures. While the range of performance does spread as the probabilities of failure are increased, there is still not a truly significant difference between the results for all architectures even when a 10% probability of failure is assumed. A probability of failure of larger than 10% per spacecraft would almost certainly be too conservative of an estimate. Therefore, the result that there is only a small difference in the performance of the architectures, in terms of this parameter, is shown to be insensitive to the uncertain input of the probability of failure per spacecraft.

5.3.1 Effect on Architecture Trade Study

The results shown above were incorporated into the TPF-I architecture down-select trade study. For the architecture down-select, each architecture design was judged based on 27 different discriminators. One of these discriminators was the ability to degrade gracefully. Each discriminator was given a weighting by a group of experts, with the sum of all weightings equal to 100 [Lay et al, 2005]. The average weighting per discriminator was therefore 3.7. Graceful degradation was judged to have an above average weighting of 4.3. The above average weighting shows the importance that was placed on this characteristic. The performance of each of the architectures was quantified using one or more parameters per discriminator, with the graceful degradation discriminator using the two parameters discussed above. The 4.3 weighting given to the graceful degradation discriminator was split equally between the two parameters.

Once weightings were set, the same group of experts judged each of the architecture's performance, in terms of each parameter. First the architecture that performed best was identified and assigned a score of 10. Next, the architecture that performed worst was identified. The group of experts then voted on the score, from 1 to 10, that should be given to the worst performing architecture. The difference in the score from the best to the worst performing architecture should reflect the difference in the level of performance, and not the importance of that parameter. The importance of the parameter was already accounted for in the previously agreed upon weighting scheme. The score given to all other architectures was then decided by a group vote. Usually, the scores for the architectures that were neither the best nor the worst performing were based on a linear transformation between the two extreme scores. The weighting multiplied by the score gave each of the architectures a particular number of points for that parameter. The points were then totaled to give the total points for each of the architectures. Since the weightings added up to 100, and each parameter was judged on a score of 1 to 10, the total number of possible points was 1000 [Lay et al, 2005].

For the overall expected percent of the nominal star-count given a probability of failure per spacecraft, the best architecture was the *Linear 3* with a value of 82%. The *Linear 3* architecture was therefore given a score of 10 for this parameter. The worst

architecture in terms of this parameter, with a value of 71%, was the *Diamond DCB* architecture. The *Diamond DCB* architecture was given a score of 7.5. All other architectures were scored based on a linear transformation between the two extremes for this parameter.

For the expected percent of the nominal star-count given a failure in a single spacecraft, the best architecture was the *X-array* with a value of 22%. The *X-array* architecture was therefore given a score of 10 for this parameter. The worst architectures in terms of this parameter were the *Diamond DCB*, the *Triangle*, and the *Linear 3* architectures. These architectures all had zero star-counts assuming a failure in any one of the spacecraft. Zero chance of any productivity given a major failure was considered a very large negative for these architectures by the group of experts, and these architectures were therefore given a score of zero for this parameter. Since the jump from no possible productive states to any possible productive states was deemed a big difference, this parameter was not scored using a linear transformation between the two extreme scores. The *Z-array* architecture, with a value of 9%, would have scored a 4.1 using a linear transformation, but was given a score of 5.0 by the group of experts. The *Linear DCB* architecture, with a value of 16%, would have scored a 7.3 using a linear transformation, but was given a score of 8.0 by the group of experts. See [Lay et al, 2005] for more details about the architecture down-select and trade study process.

The difference in performance across architectures, in terms of the expected percent of the nominal star-count given a failure of a single spacecraft, ranged in scores from 0 to 10. Given a sub-weighting of 50% of the total weighting of 4.3, or 2.15, this corresponds directly to a point difference as high as 21.5 points. This difference had a significant impact on the outcome of the trade study and the down-select. As an example, a 20 point difference between the *Linear DCB* architecture and the *Z-array* architecture can be attributed exclusively to the graceful degradation discriminator (both parameters). This difference is especially large when considering that the total point difference, considering all discriminators, between the two architectures was 31 points. This example shows that the graceful degradation discriminator was not only given a

high importance weighting by the group of experts, but also made a significant difference in the outcome of the architecture down-select and trade study.

5.3.2 Design Change Due to Study

In addition to affecting the outcome of the architecture down-select, the graceful degradation study presented here also affected the design of the possible TPF-I mission architectures. The *Linear DCB* and the *X-array* architectures have similar beam combiner designs. The beam combiner is the part of the instrument that combines the beams from the separate spacecraft and finds nulls. The design of the beam combiner is a large part of the experimental and theoretical work that has been ongoing for TPF-I. While there are initial sketches and theoretical designs for a beam combiner for each of the architectures, most of the effort has focused on designing the beam combiner for the *Linear DCB* and *X-array* architectures.

Prior to the work done in this study, the design under development for the beam combiner did not easily support adding in the ability to vary the phases of the beams. While the design team was developing a single design in detail, prior to choosing the given design, a trade study was done and several designs for the beam combiner were considered. The ability to vary the phases of the incoming beams was not considered as a parameter when choosing a beam combiner design, since at the time there was no need to vary the phases. However, one of the designs under consideration that was not initially chosen to be developed in detail could easily support adding the ability to vary the incoming beam phases. Therefore, after reviewing the results of the graceful degradation study, and learning that being able to operate in a degraded state after the loss of a single spacecraft both would be possible, and would be considered high priority among experts, the lead engineer in charge of the beam-combiner design suggested switching the baseline design, to consider in more detail the design that could accommodate varying phases.

This suggested design change materialized because a study was carried out, very early in the development cycle of the TPF-I mission, to examine what would be required

to be able to operate in degraded states, and how productive those degraded states would be. It was discovered that, with a design change to allow for variable phases, several of the mission architectures could operate in a degraded state without a single spacecraft. The productivity in these degraded states proved to be enough to merit the change in design, as seen both in this study as well as in the TPF-I Risk Analysis study shown in Chapter 6. While this design change is relatively small at this point in the development cycle, it may have been impossible to make such a change later. If these same results had not been shown until several years later in the design process it would have been impossible to change the design of the beam combiner. The design that does not support variable phases would have been worked out in detail, and switching to a new design would have required a very large amount of effort and resources. A cost-benefit analysis at that point in time would almost certainly show that it would not be worth switching designs to achieve the extra risk mitigation and benefits accrued from having variable phases. The cost of making this same design change at the current point in the development cycle for the TPF-I mission is significantly smaller in terms of effort and resources. Therefore, it is worth it from a cost-benefit stand-point to make this design change while in this early phase of the mission. By conducting the degraded state study early enough in the life-cycle of the design process, it is possible to affect the design from the early stages, when design changes are not as costly. We are more likely to achieve a design that is inherently robust and low risk if we allow risk to be a tradable parameter throughout the design process, instead of simply a parameter that is calculated when the design is completed.

5.4 Conclusions

This case-study showed the method behind, and results of, a study to determine possible degraded states for various TPF-I architectures. Rules for determining the productivity of a degraded state were determined. The productivity in these degraded states was then quantified using two separate parameters, to bring risk and the concept of graceful degradation directly into an ongoing architecture trade study and down-select for a real NASA mission, TPF-I.

This graceful degradation case-study showed the impact that a risk-based study can have on the design of a mission if carried out early in the design life-cycle. The design of the TPF-I mission was affected by the results of this case study in two separate ways. First, the architecture selection was directly affected by the varying architectures ability to degrade gracefully. Second, a major design change to the beam combiner was recommended, to allow for risk mitigation and graceful degradation. These two impacts directly show how incorporating risk into the design process at an early stage can, and did, have an affect on the design of a flight mission.

Chapter 6

CASE-STUDY 2: RISK MODEL AND ANALYSIS FOR TPF-I

6.1 Introduction and Motivation

At the end of the architecture down-select process discussed in Chapter 5, the TPF-I design team chose the *Linear DCB* architecture as the baseline design. Once this architectural design was chosen, more detailed design work could begin. A more comprehensive risk model and analysis was among the studies that were completed.

While the degraded state analysis discussed in Chapter 5 used expected productivity analysis to determine the risk of various TPF-I architecture designs, it was not a detailed risk analysis. The purpose of the degraded state analysis was to determine the *relative* risk of each of the possible architectures, in terms of major failures only. The study was limited to the impact of failures of full spacecraft, and did not explore how or why the spacecraft may fail. Once the baseline design for the mission was chosen, it was possible to begin a much more in-depth risk analysis. In this case, the specific risks and failure modes for the *Linear DCB* design were examined.

The risk analysis process for TPF-I consisted of three major steps:

1. Capture and define the major risks associated with TPF-I.
2. Create a model of the risks to determine the effect on the mission productivity.
3. Analyze and compare the risks.

Each of these steps will be discussed in detail in the following sections.

6.2 Capture and Define Risks

The first step in developing any risk model is to gather the information required about the risks to the project. This has been accomplished for TPF-I by interviewing several experts from the TPF-I design team. Examples of the type of questions asked during the expert interviews include:

- *Describe your subsystem. How does it work? What does it do? What are the major attributes?*
- *What are the most probable failure modes for your subsystem? The most catastrophic?*
- *What are approximate probabilities of occurrence for each of the failure modes discussed? What are the impacts on the mission if each failure were to occur?*
- *Does your subsystem depend on any other subsystem?*
- *Are there any technologies being developed that would help to mitigate the risks discussed?*

It should be noted that while these are examples of the types of questions asked, not every question was asked to every expert. The interview questions guided conversation, but were not strictly followed.

Eleven interviews in total were conducted, with experts from the attitude control system (ACS) [Rahman, 2003], structures [Adams, 2003], the Autonomous Formation Flight (AFF) sensor system [Tien, 2003], formation flight algorithms and control [Ahmed, 2003], the instrument system [Martin, 2005], and six systems level experts [Fisher & Miller, 2003] [Gunter, 2005] [Hamlin, 2005] [Henry, 2005] [Lay, 2005]. These interviews resulted in 101 risk items. A risk item is defined as either a failure mode or a development risk. A failure mode is a failure that could occur once the system is designed or built. An example of a failure mode is a deployment failure. A development risk is a risk that a given aspect of the design will not be developed in such a way as to meet requirements, even in a nominal state. An example of a development

risk is the possibility that a material will not be found that is capable of remaining stable enough to meet requirements at cryogenic temperatures.

After reviewing all risk items captured during the interview process, three major categories of risks were identified. These categories were:

1. Risks that result in the failure of a single spacecraft
2. Risks that result in the failure of the entire system or constellation
3. Technology development risks

Additionally, the risks that result in failures of either the individual spacecraft or the entire system could be broken down further. Failures of the individual spacecraft fell into categories of bus failures, payload failures, or the Autonomous Formation Flight (AFF) system failures. System level failures could be broken down into systematic bus failures, systematic science or payload failures, formation failures, control system failures, or failures that occurred prior to the beginning of operations, known as pre-operations failures. All categories of risk items can be seen in Figure 6-1.

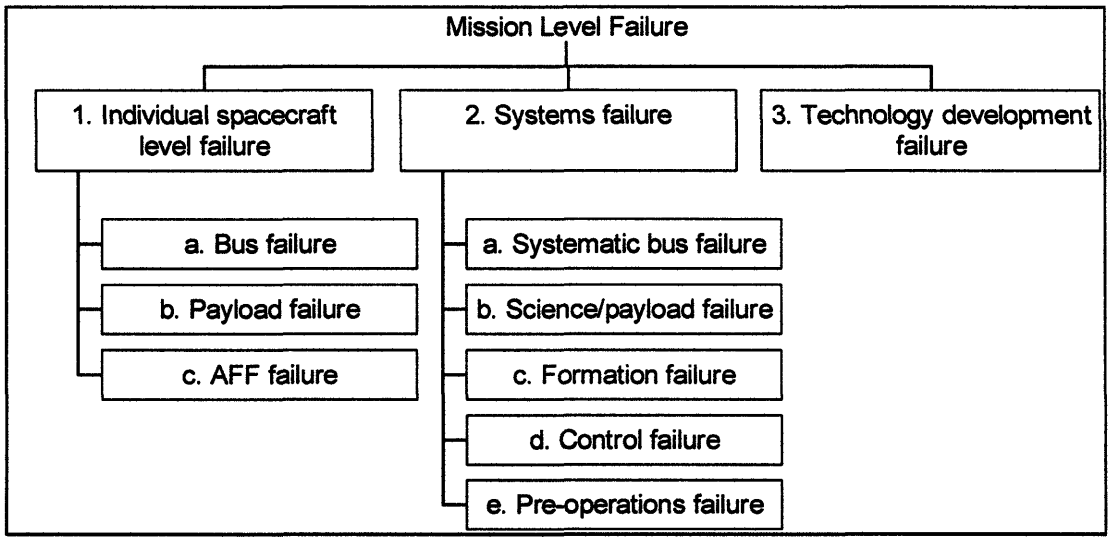


Figure 6-1: Categories of risk items.

Each development risk or failure mode was placed into one of the categories discussed above. Several of the risks or failure modes captured were clearly sub-sets of other risks or failure modes. It is important to keep the level of the risk identifiable. In other words, a failure of the entire spacecraft would not want to be placed on the same level as a failure of a particular actuator. A tree structure was implemented to capture this idea of risk levels. As an example, two ways that the payload could fail would be if the optical delay line (ODL) failed or if the starlight camera failed. The ODL itself could fail due to a failure in the ODL sensors, the ODL actuators, the ODL cryo-coolers, the ODL interface hardware, or the ODL software. Therefore, an ODL sensor failure is a level below the full ODL failure, and the full ODL failure is at the same level as a starlight camera failure. This results in a risk list with a tree structure. A higher level failure could occur from any one, or multiple, of the lower level failures.

It is important to note that the tree-structure and categories discussed above are for organizational purposes only. They are used to help organize the list of risk items and to clarify the risk list when showing design team members and managers. The categories and tree-structure do not affect the results of the risk model, in terms of the expected number of observations completed.

The full TPF-I risk list can be seen in Appendix A. The following sections describe the risks to the TPF-I mission, organized into the categories discussed above, and shown in Figure 6-1.

6.2.1 Individual Spacecraft Failures

6.2.1.1 Individual Spacecraft Bus Failures

Bus failures include all failures that result from non-payload related engineering functions. These risks are not specifically related to the interferometer instrument. What makes TPF-I unique in terms of these risks is the fact that the functions are required across five different spacecraft.

Deployments are one of the riskiest aspects of any space mission. This particular mission has a very large number of deployments, many of which are single point failures. In addition, deployments tend to be looked at as "something that's been done before". Therefore, in a mission such as this one, with many aspects that haven't been done before, there is concern that deployments may be overlooked.

There are a relatively large number of deployments per spacecraft – causing significant risk to each individual spacecraft. The four main deployments on the buses are the sunshades, the solar arrays, the high gain antenna, and the cryo-radiator deployments. There are six cryo-radiators and four solar arrays per spacecraft that need to deploy. The sunshades need to deploy on each spacecraft in order to achieve the thermal environment required. While the exact deployment sequence for the sunshades has not been developed yet, this sequence may include several stages, including folding out or deploying booms, and deploying a spreader to provide the correct angular separation between the layers of the sunshade. The high gain antenna, located only on the combiner, will also need to be deployed.

A meteoroid or other debris strike is also of concern to all space missions. These types of strikes are particularly concerning for TPF-I due both to the surface area, and the sensitivity, of the spacecraft. With 4m diameter mirrors and 4 apertures, there is 50 m^2 of mirror surface alone that is in danger of strikes. The impact of a meteoroid or debris strike can vary from no damage to catastrophic based on several variables, including the size and location of the strike. If a meteoroid were to hit one of the apertures with enough force to cause damage, the effect could range from impacting the optical surface of the mirror to a catastrophic failure. If the strike were to leave a spot on the mirror, this would in effect reduce the effective collecting area of the aperture, but would not cause the aperture to no longer function. The question in this situation is whether or not the interferometer can deal with apertures with different optical surfaces. A hole in an aperture would be more of a catastrophic strike, as this would cause stray-light issues, in addition to the same sensitivity issues (reduction in collecting area). For this study, it is assumed that a meteoroid strike to any spacecraft would result in the complete failure of that spacecraft.

At the time of operations for TPF-I, there is the possibility that several other missions, such as WMAP, SIRTF, and JWST will also be in orbit about L2. There is the slight possibility that, due to a control error from either TPF-I or one of the other missions, one of these other spacecraft could impact the TPF-I spacecraft. If this were to occur the effect would almost certainly be catastrophic, however the probability of this occurring is so low that it is still considered a very minor concern.

TPF-I will rely on computers and autonomy algorithms for operation. Computers will be required to find and track any fringes. Therefore, a computer failure would be catastrophic. However, computer designs meant to sustain the radiation environment at L2 have been flown before, and will be flown many more times before launch, leading to an extremely low probability of a computer failure.

The Attitude Control System (ACS) is responsible for maintaining the attitude of the spacecraft. This subsystem ensures that the spacecraft remain correctly oriented with regard to the star, and to the other spacecraft. The system will use star-trackers, gyros, and sensors. All of these components have some possibility of failure.

The Direct-to-Earth (DTE) communications capability aboard the combiner spacecraft could also fail. While all five spacecraft will contain some DTE communications capability, the DTE capability aboard the collector spacecraft will be significantly reduced compared to the combiner spacecraft. Therefore, if the DTE capability aboard the combiner spacecraft is lost, the system would be in a degraded state.

6.2.1.2 Individual Spacecraft Payload Failures

The instrument system is in charge of designing and building the interferometer instrument. This includes both the collecting and combining aspects of the system. The majority of design work at this point has been conducted on the aspect of combining the beams of light to find fringes.

One of the biggest challenges for TPF-I, in terms of risk, is the very large number of mechanisms on each spacecraft payload. There are four alignment mirrors inside the combiner. Each collecting spacecraft has an actuated field of regard mirror, a mirror to allow the metrology beam to align with the starlight beam, a transfer mirror, and a wave-front sensor. Each inner collecting spacecraft also has an additional moving mirror with sensors. The beam combiner also has an additional two alignment mirrors per starlight beam for the metrology beam alignment. Finally, each collecting spacecraft has a single alignment mirror to adjust for the secondary mirror deployment. This mirror will move once and lock into place, so it should have only a single event failure mode.

One of the main components to the instrument system is the optical delay lines. The delay lines have some redundancy built in. There are 4 sets of delay lines on the combiner, and only 3 are theoretically required for interferometry - one delay line for each pair of beams (2 total) plus one for combining the pairs. All beam paths are identical, so a failure in any single delay line should result in a functioning system, with a layer of redundancy removed. There are 5 total stages of actuation in each delay line – one course stage, two voice coils, and two piezo stages. In addition to the actuation stages, the delay lines also contain sensors, interface hardware, cryo-coolers, and software.

There are several simple sensors throughout the system that should be reasonably robust. However, there are additional more complex sensors that may have a higher probability of failure. These include the science and fringe tracking cameras. There are two fringe tracking cameras and a single nulling, or science camera. These cameras are not redundant, such that all three are required for a functioning system. There is no room to put a redundant camera system of either kind. In addition to a complete failure, any of these detectors may also be less sensitive than was expected prior to launch. One possible source for decreased sensitivity in the detectors would be radiation damage. Decreased sensitivity of a detector is a degraded state since, assuming it can be calibrated for, it is possible to adjust for the decreased sensitivity. This degraded state would have increased calibration and observation time over the nominal state.

The metrology system consists of 13 fast steering mirrors spread out over 5 spacecraft. Additionally, 9 intensity gradient detectors (IGDs) are required to control the fast steering mirrors, which essentially control the starlight angle. These sensors have no moving parts and are assumed to either work or not work, but will not fail throughout the lifetime of the mission. Metrology alignment mirrors are needed to control the path-length from internal variations. Finally, two metrology lasers are required for the system to work. All elements are single point failures, and there is no clear method to put redundancy into the system.

Every mechanism in the optical train is a single point failure. Stationary optical elements could get damaged, such as a misalignment at launch, and cause a single point of failure. The bigger concern, however, is with moving parts of the optical path, such as fast steering mirrors, actuators, and delay lines. If any of the mechanisms allowing motion in these components fails, the whole system fails. In general, moving parts are a cause for concern for spacecraft designers, but in this case there is even more concern due to the number of critical moving parts that need to not only function, but also function accurately and smoothly. Note also that these moving components may fail due either to not surviving launch or to wear and tear. Many of these components will be moving at 100 to 1000 Hz, which may cause additional stress.

As with the buses, the individual spacecraft payloads also require deployments. These fault modes consist of a failure during the deployment of the stray-light baffles or the secondary mirror. There are a total of ten stray-light baffles across all spacecraft that need to be deployed. The secondary mirror is the most critical, and therefore the most dangerous, of the deployments. The secondary mirror needs to be deployed precisely and then held stable at cryogenic temperatures. The deployment is an especially difficult deployment since the positioning needs to be extremely precise. A lock-out deployment will probably need to be used to ensure this precision. A failure on deployment of the secondary mirror would lead to a complete failure of that particular telescope. If the system could operate without that telescope, this particular failure may not be a complete system failure however. Finally, it is possible that a mechanism that locks down the

optical components for launch may not release, or deploy, and would cause a failure of that spacecraft.

The mechanism to include variable phases, which allows for degraded states with one fewer spacecraft, could fail. Two mechanisms are considered: the first uses wedges sliding across one another with a motor, and the second uses rotating plates also driven by a motor. There is some possibility that the mechanism could get stuck in one end point or another, but the design is well understood, and the probability of a failure is very low. It may also be possible to add redundancy to this mechanism to additionally reduce the probability of failure.

The high-low resolution switch could also fail. This would result in the system being stuck in either the high or low resolution mode. It is also possible for this switch to fail such that neither position could be reached, leading to complete system failure.

While ground testing can lead to a reduction in several risks, it can also lead to additional risks. Modifications will need to be made to the flight system for ground testing, to account for differences in the environment and test set-up. While many of these modifications will be accomplished through software, one hardware modification is required. To test the internal beam path for the combining spacecraft, mirrors will be placed over the input channels. A test beam will then be sent from a source in the middle of the combining bench through the internal beam path, reflect off the mirrors, and return through the beam path to the detectors. If these test mirrors are not removed, or if the mechanism to move these mirrors fails in the down position, there would be no input capability to the combiner.

The cryo-cooler is used to bring the optics down to the required temperature. A failure in the cryo-cooler would result in a significant increase in the temperature of the optics. An increase in the temperature of the optics of more than a few degrees translates directly into a critical increase in the noise level. Therefore, it is assumed that a failure of the cryo-cooler would result in a failure of the mission.

To achieve the correct signal to noise ratio and light-collecting capability, there are requirements placed on the quality of both the primary and secondary mirrors for all collecting spacecraft. If any of the mirrors do not meet these requirements, collection ability of that particular spacecraft would be lost. Note that this failure mode affects a spacecraft's ability to collect light, but not the ability to transfer beams.

The final two risks regarding the payloads on the individual spacecraft both involve control. There is a risk of loosing control of the secondary mirror. This would result in a lack of the ability of that particular spacecraft to do wave-front control, and therefore a lack of the ability to collect starlight. There is also a possibility of contamination of either the primary or secondary mirrors due to a control system error. In this failure mode one spacecraft would be erroneously sent a command to fire thrusters toward another spacecraft. This risk does not cover the failure mode that nominal operations, with all spacecraft in the proper orientation, causes contamination. Nominal operations contamination would be systematic, and is therefore covered in the systems-level science section.

6.2.1.3 Individual Spacecraft AFF Failures

The Autonomous Formation Flight (AFF) system is the course knowledge sensor for formation control. For TPF-I to be able to hold a formation, requirements are placed on both knowledge and control. The AFF system is in charge of the knowledge portion of these requirements. The system includes 4π steradian coverage and close range radar capability for collision avoidance.

The AFF system hardware includes 4 transmitting antennas, 12 receiving antennas, 4 transmitter modules, 12 receiving modules, 1 baseband processor, 1 frequency subsystem, and 1 power subsystem. While they aren't a part of the AFF sensor system, actuators use the knowledge provided by this system to move the spacecraft and hold the formation. The actuators are therefore also placed in this category. There are also software components to the system which are used to control the sensors. The

software component risks are common across all buses, and are therefore discussed with the systematic bus failures.

There are multiple catastrophic AFF system failures. There is only one each of the reference signal and baseband processor. These items are single string and the course sensing system would be lost if either of them failed.

There are several additional degraded state failures for the AFF system. If up to two antennas or transmitters fail, it may be possible to still get some coverage. Some parts of coverage are more critical than others. This could lead to different levels of degrading failures. A partial failure of the AFF system would cause the probability of collision between spacecraft, and of formation evaporation, to increase.

6.2.2 Systems Failures

Systematic failures are failures that affect the entire system. If any of these failures or risk items occur the entire system, including all five spacecraft, would be affected at the same time.

6.2.2.1 Systematic Bus Failures

The ACS subsystem was discussed above in the individual spacecraft bus section. While the different hardware components for the ACS subsystem are on each spacecraft, and could therefore fail individually on each spacecraft, the software, or estimation function, for the ACS subsystem is identical for all spacecraft. Therefore, a software error would be a systematic error, and would most likely cause a failure of all five spacecraft.

The thermal subsystem is also a concern. There is a possibility of leaks from the warm side to the cold side of the spacecraft. Given the uncertain nature of the thermal system, it is possible that these leaks may be missed prior to launch due to a lack of the ability to completely model, or measure, the thermal characteristics of the system.

Sources for thermal leaks include a lack of appropriate thermal shielding, power or electrical lines, or simply excess sources of heat on the cold-side of the spacecraft, possibly due to the placement of other sub-systems. An increase in the temperature of the optics would result in an increase in noise for the observations. It has been approximated that an increase of only a few degrees on the optics will result in approximately twice the noise factor for observing. Therefore, it is assumed that with only a single source of thermal leaks the system could still function, but in a degraded state. It is assumed that if multiple thermal leaks were to occur, no observing would be possible.

If the thrusters used on all spacecraft are not modeled or tested properly prior to flight, the out-gassing rate may be higher than expected. While this could be accounted for through adjustments made during operations, it would result in a higher rate of fuel consumption than planned. This would lead to a shorter lifetime than in the nominal case due to a lack of consumables.

In addition to the hardware errors discussed above, operator errors are also a concern. An example of an operator error would be sending a command to the wrong spacecraft. Operator errors are considered a system level concern, since the operator is in charge of the entire system of multiple spacecraft, such that an error in any single command would most likely affect the entire constellation.

6.2.2.2 Systems Science or Payload Failures

The possibility of receiving bad data from the instrument is a concern. It is unclear how TPF-I protects against bad data. In other words, how does one verify what the observatory is seeing? With no method of verification this is a very risky area for TPF-I. Possible sources of bad data include an exo-zodi with lumps, contamination of the spectra from hidden planets, or a failure of the planetary signal extraction algorithms.

Even without the consideration of bad data, there are still risks involved in the observing scenario for TPF-I. If the formation control is not as accurate as desired, or if the formation can not be stabilized to the desired level, it will be difficult to achieve

sufficient observing time between movements. The number of calibrations required may also lead to a lack of stable observation time.

In addition to the risk of contamination from a control system error discussed in Section 6.2.1.2, there is also a risk of contamination from thrusters during nominal operations. If testing and modeling are incorrect or inconclusive, it is possible that the mirrors of the collecting spacecraft could be contaminated either by their own, or neighboring, thruster plumes. Since this situation would occur due to a systematic design flaw, this risk affects all the collecting spacecraft in the system.

As discussed previously, the optical path for this system requires very high levels of precision and accuracy. Any misalignment of the optical path elements could result in mission failure. One possible source of optical misalignments is from thermal variations. While these thermal induced optical misalignments would be small enough that they could be calibrated for in most circumstances, they would result in extra calibration time, which can be modeled as a decrease in the lifetime of the observatory. There would also be situations in which enough control authority would no longer exist in the delay lines to remove certain disturbances. This situation can be modeled with decreased observational efficiency, since the extra disturbances will result in more overhead time.

Stray-light is a major concern for the TPF-I design team. Modeling is used to determine the causes and effects of stray-light on the observatory system. This modeling results in recommendations of how to mitigate stray-light. Examples of stray-light mitigations include using stray-light baffles at all beam input and output locations on the spacecraft, and restricting the spacecraft to flying within a maximum distance apart to reduce beam spread. The results of these stray-light models set the size of the stray-light baffles and the maximum distance apart the spacecraft are allowed to fly. If the models have either missed or underestimated any sources of stray-light, these mitigation techniques may not solve the problem. Depending on the severity of the stray-light issue, this could result in either decreased observational efficiency, or in mission failure.

The metrology system is used to measure the path-lengths of the science beams. If the metrology beam has a slight misalignment from the science beam, and this

alignment is not sensed by the metrology system, a path-length error will occur. This situation is called beam-walk, and results in complete system failure.

6.2.2.3 Systems Formation Failures

The formation flight system is responsible for the knowledge and control of the inertial attitude of each spacecraft, the relative range and bearing of all pairs of spacecraft, the formation pointing capability, and the corresponding rates to all of these. The goal for knowledge of the relative range is at the single centimeter level, while the goal for relative bearing is at the single arc-minute level. The goal for control is 5-10 centimeters, and 5-10 arc-minutes, respectively. While these goals may be able to be met currently with state of the art technology in the laboratory for individual spacecraft, formation control and knowledge are much more difficult for constellations of spacecraft.

There are two types of failures of the formation flight system – failures which affect only the local, individual spacecraft, and failures which affect how the spacecraft will react in the formation. Failures to individual spacecraft are covered in Section 6.2.1.3. Two of the most likely failures modes of the formation from a system level include the collision of two or more spacecraft and evaporation. Evaporation occurs when the spacecraft loose formation by drifting more than 10km apart from one another. Either of these failure modes would be catastrophic.

The most difficult and challenging part of the formation flight system is the new software design that is required, including signal structure, processing algorithms, and frequency subsystem design. This is due to the requirements placed on the system from the simultaneous operation of multiple spacecraft. One of the major error sources for the system comes from multi-path. Multi-path occurs when a signal bounces off another spacecraft instead of coming directly from the originating spacecraft. A failure of the AFF software structure would be catastrophic.

The handoff between the course to medium sensors, and medium to fine sensors, could be a concern. There is no real way to test this handoff accurately, and the analysis and modeling is not at the level it needs to be at as yet.

The formation flight algorithms rely on very fast inter-spacecraft communication. If there is a failure of the inter-spacecraft communication system, the individual spacecraft would not be able to determine where each of the other spacecraft is, resulting in a formation failure. In addition, if there is too much latency in the communications system, the formation control would be very difficult.

The process of acquiring the formation for the first time is also risky. After deployment from the cruise stage, the individual spacecraft need to turn on the AFF system, acquire signal from each of the other spacecraft, and maneuver into an initial formation. All of these steps need to be completed before the spacecraft either collide, or drift apart beyond the sensor range. While the end result of this failure would be collision or evaporation, it is a separate risk item since the cause of the failure is unique.

6.2.2.4 Control Failures

One of the main sources for concern regarding the control algorithms for TPF-I is the possibility of vibrations on the spacecraft due to self-induced disturbances. There are five primary excitation sources on the TPF-I spacecraft – the cryo-pump, the reaction wheels, the thrusters, moving optics, and thermal snap. Thermal snap occurs since the spacecraft needs to rotate to observe, and is therefore in a continuously varying cone angle from the sun. While thrusters will certainly cause vibration issues, it is hoped that the thrusters will only be used when absolutely necessary, such as to de-saturate the reaction wheels, but will not be used during observations. Moving optics, such as delay lines, will need to move throughout the observing process, however. The final source of self-induced vibrations is a disturbance from the placement of other subsystems. Solving the vibration problem is difficult since you need some control in order to correct for any vibrations that do occur, but the more powerful a control system you have, the more vibrations you are likely to excite with it. Whether or not science could be collected in

the presence of vibrations given an excitation failure would depend on the level of vibrations. Science return would definitely be reduced however.

Another possible failure mode is sensor noise coupled into the control loop. The possible noise sources for TPF-I have not been characterized to the level needed to integrate into the design process. Characterizing these noise sources is a work in progress.

The control system relies on the propulsion system to provide all 6 degrees of freedom whenever needed. There is a concern that the control loop will need to thrust in a given direction, and won't be able to because of plume impingement risks, or hardware in the way. This would result in thrust directions being limited, causing control difficulties.

A degraded state is also possible from plant dynamics changing, due to fuel slosh or fuel usage. This would cause the control to be more difficult, and would affect the observational efficiency.

The final control system risk item is the risk of an un-sensed mode. This is the risk that there is collector vibration, in the direction of the star, at a frequency higher than the fringe tracker can measure, or approximately 1 Hz. Since this mode would be un-sensed, it would also be impossible to track, leading to a failure to track the fringe.

6.2.2.5 Pre-operations Failures

Launch failures are something that all spacecraft need to worry about. However, nothing is unique about this particular launch that makes it more risky than other launches. The current design is slated to use a Delta IV heavy rocket. It is unclear how many of these rockets will have launched previous to TPF-I. A failure during launch would almost certainly be a complete failure.

Additional launch failures consist of scenarios such as a piece of the spacecraft breaking, or experiencing permanent deformation, due to launch loads. To protect

against this type of failure the design is analyzed to ensure it is strong enough, stiff enough, and has enough damping to survive the known launch environment. The acceleration loads placed on the system at launch could also cause failures or misalignments.

This mission consists of a more complex system of systems than the engineers and designers are used. Additionally, it is impossible to test the full observatory system during ground testing. The complexity of the system, coupled with the lack of the ability to fully test the system on the ground, increases the number of unknown unknowns. The high level of complexity also leads to an additional risk of design error, or incorrect requirements.

While it will not be possible to test the full observatory system on the ground, as much ground testing as possible will be carried out prior to launch. Mishandling during ground testing can also be a concern. Lack of testing can lead to certain risks, but increased testing can also lead to risks of failures occurring during testing.

Missing the L2 injection has a low probability, since this problem has been done before, and will be done several more times before TPF-I flies. The James Webb Space Telescope will be a good risk retirement vehicle for this particular risk.

A failure during cruise stage would be mission catastrophic. However, this phase of the mission is essentially the "easiest" phase of the mission – with nothing new being done for the first time. In addition to having heritage to previous designs, there will also be fault protection built into the cruise stage that should remove the majority of the risks involved in this stage, such as a propellant failure during a mission critical maneuver.

The deployment of the constellation from the cruise stage is also a concern. The exact deployment sequence is not known at this time, but more than one deployment may be required. Tip-off during spacecraft deployment could be a relatively major issue. This would occur if there is contact with the cruise stage during the deployment of any of the spacecraft, due to unbalanced spring forces.

6.2.3 Technology Development Failures

Developing the instrument control technology such that it can meet the requirements is an area of concern. The requirements on TPF-I are much tighter than those that were placed on a previous NASA formation flown interferometer mission, Starlight, which were already challenging to meet. The current requirements for TPF-I are to cover 10 arcminutes over a 10 milliarcsecond resolution. This leads to a dynamic range of 60,000. While this requirement would be exceptionally difficult to meet, it is still very preliminary. If the resolution or range could be relaxed, the requirement would be much easier to meet. An estimate of a dynamic range that could be realistically met would be approximately 6,000.

Keeping the spacecraft structure stable, with very little vibration, is especially difficult at cryogenic temperatures, since the characteristics of materials are somewhat unknown in this temperature range. In addition, in most common materials as the temperature decreases, the amount of natural damping in the material also decreases. Therefore, it has been theorized that these materials will ring for a very long time when placed in a cryogenic environment. While the exact problem is not well understood, since cryogenic structures are not well understood on a large scale, it is theorized that this is a problem which is orders of magnitude worse than the same excitations would create in a room temperature environment.

A testing program to examine the characteristics of cryogenic structures would greatly help with the stability failure mode. This testing could be done on ground or with the shuttle, with more accurate testing available from the similar environment of the shuttle. Ground testing may be possible but will be difficult. Testing would definitely help to understand the problem better, which would in turn help with understanding the solution. Sophisticated modeling efforts could also help the stabilization issue. These models should simulate the environment and the spacecraft. Finally, tasks are underway to develop new materials that have more natural damping in cryogenic temperatures. One material that is looking promising is a version of a glass. There appears to be more possibility of finding better materials for the mirrors of the telescope than for the structure, although the search is still on.

For the formation system, the technology to develop the AFF sensors to produce 4π steradian coverage without requiring any maneuvering is at TRL 3-4. The technology to develop smart algorithms to avoid collision is at TRL 5-6. Finally, the technology to develop on-board autonomy for formations is at TRL 3. In all cases the ideas for how to accomplish the tasks are there, and just the resources and time to develop them are required.

There are two main technology developments for the instrument system. Single mode spatial filtering uses optical fibers to filter the wave-fronts. Wave-fronts from the different apertures are distorted in different ways. The single mode filter is blind to the details of the distortion and simply takes the average. This technology leads to the ability to match wavelengths and relaxes the requirements on optical alignment. The other main technology development is adaptive nulling. While this technology development is proceeding well, it should be noted that it is a key, required technology.

There is a concern of trying to control a formation of spacecraft in the unstable environment of L2. Some technology will need to be developed to both model this unstable environment to the level needed, and to develop the control algorithms required for this environment.

Finally, as discussed previously, it is important for the formation flight control that the inter-spacecraft communications meet given latency requirements. While the basics for the inter-spacecraft communications system exist, this latency requirement will require new technology development.

6.3 Risk Model

Once the risks were identified through expert interviews, the process of developing a risk model began. Each risk item required two main components to be modeled – probability of occurrence, and impact in the event of occurrence. All impact and probability information was based on a combination of engineering judgment and expert opinion. An effort was made to ensure consistency across the model when dealing with varying experts opinions.

6.3.1 Impacts

There are two main categories of impacts for risk items – those leading to complete failure, and those leading to a degraded state. Risk items that lead to degraded states can lead to any of the following states:

- Loss of a spacecraft
- Loss of a spacecraft payload
- Reduced observational efficiency
- Increased failure rate of a different failure mode
- Reduced lifetime
- Increased integration time
- Increased minimum baseline length
- Decreased maximum baseline length
- Stuck in the high or low resolution mode
- Stuck in the three-collector or four-collector mode
- Combination of above

If the risk items that lead to the loss of a spacecraft occur on one of the outer collecting spacecraft, the system is still able to function using the remaining spacecraft. If these risk items occur on one of the inner collecting spacecraft, or on the combining spacecraft, the system would not be able to function, since there would be no way to get three star-light beams with equal path-lengths to the combining spacecraft. An example of a risk item that leads to the loss of a spacecraft is a failure of a component in the specific optical path of each spacecraft.

Loss of a spacecraft payload is defined as the loss of the collecting ability of one of the collecting spacecraft. A loss of an outer collector spacecraft payload results in the same degraded state as a loss of the entire outer collector spacecraft. A loss of an inner collector spacecraft payload results in a degraded state in which the inner spacecraft can not collect light, but can still transfer star-light beams from a different collector to the combiner. Therefore, a loss of an inner collector spacecraft payload can still lead to a

degraded state with three collecting spacecraft, as long as all other spacecraft and payloads are still functional. A secondary mirror deployment failure is one of the failures that would lead to the loss of a spacecraft payload.

Reduced observational efficiency is one of the most common impacts of risk items. Observational efficiency is defined as the ratio of time spent observing to total time. The total time is the observing time plus the time required for overhead, including all engineering and house-keeping functions. The observational efficiency is usually decreased due to an increase in the required overhead time per unit of time spent observing. This can occur if more engineering functions are required, or if these functions would take longer, given a particular failure. One example of a risk item that leads to reduced observational efficiency is if plume impingement concerns restrict the possible thruster firing directions for the control algorithms.

Another very common impact for risk items is the increased probability of a different failure mode. One of the more common failure modes impacted by other failures is a collision of spacecraft. The loss of a single sensor in the AFF system will not result in system failure, but will result in an increased probability of a future collision. Other common failure modes that are impacted by other failures are evaporation, and not having enough time between disturbances to settle the spacecraft to the required level.

Reduced lifetime can occur if more time is required for calibrations, or if consumables are used at a rate higher than expected. An example is if the thruster out-gassing rate is higher than expected. This leads to a shorter lifetime because of the limited amount of fuel available.

The integration time per star is a function of the signal-to-noise ratio of the instrument system. Therefore, an increase in noise levels will lead to an increase in integration time per star. As an example, a single thermal leak to the cold-side of the spacecraft would result in an increase of a few degrees of the temperature of the optics. This increase in temperature would correspond directly with an increase in noise, which corresponds directly to an increase in integration time.

The distance between the individual spacecraft in the formation sets the baseline distance for that formation. The baseline determines the resolution of the instrument. In some cases a longer baseline is required, while in other cases a shorter baseline is required. See Chapter 4 for a review of how the baseline affects the observational ability of the instrument. The minimum distance between any two spacecraft in the formation is set for safety reasons, to avoid collisions between spacecraft. Failures of the AFF system to perform as required could lead the design team to decide to increase the minimum allowable separation distance between spacecraft. The maximum separation distance is set by stray-light concerns, and is only applicable to spacecraft between which a beam is being transferred. If a single stray-light baffle were to not deploy, the system could still function, but the maximum allowable distance between spacecraft would be decreased. Note that in some cases, depending on which spacecraft the failure occurred on, it may be preferable to use only three spacecraft, but use the nominal maximum allowable distance. This is accounted for in the model.

The final two possible impacts are specific to given risk items. If the switch that determines if the system is in high-resolution or low-resolution mode is stuck, the system will clearly be stuck in one of the two modes. Similarly, if the mechanism to allow for variable phases becomes stuck, the system could be stuck in either a three or four collector mode.

6.3.2 Probability of Occurrence

It is very difficult to determine the probability of each of the risk items occurring. An initial attempt was made to determine the probability of occurrence from the expert interviews that provided the risk items. It became clear however, that not only was each expert uncertain in his or her response, but responses between experts were not correlated. The optimistic versus pessimistic stance of the individual expert led to a very wide range in the value of probabilities. Therefore, it was decided to set the probabilities using bins of values. Five probability bins were used – very high, high, medium, low, and very low. Determining which category, or bin, a given risk item fell into was much

more intuitive to the experts interviewed. Each probability bin was then given a specific probability value. Probability values of 10%, 5%, 1%, 0.5%, and 0.1% were used for the very high, high, medium, low, and very low bins respectively. If a failure mode or risk item could occur at any point throughout the lifetime of a mission, such as the failure of a moving component or part, this probability value was used as the probability of the failure occurring by the end of life. An exponential failure rate was then calculated using this probability.

In order to normalize the probabilities between experts even more, a set of group definitions was determined to assign a probability bin to each risk item. These groups were based on the reasoning that the experts gave as to why certain risk items fell into a particular bin. As an example, it was determined, through expert interview, that a deployment failure of the secondary mirror is more probable than any other deployment failure, since a very high precision deployment is required. Therefore, separate groups were defined for general deployments and for precision deployments. The description of each group, along with the probability bin and value assigned to that group, is shown in Table 6-1.

In a few cases a known, unique probability value was given to a risk item. This occurred in three cases. The probability of being hit by a micro- meteoroid while in orbit about L2 was based on research done for the James Webb Space Telescope in 1998 by Lindsey [Lindsey, 1998]. The value used was the sum of the flux per square meter of meteoroids between 0.5 cm and 7 cm in diameter, times 5 years of operation. This value was then multiplied by the exposed surface area of TPF-I, including apertures and sunshades. The same value was used to determine the probability of hitting another mission in L2. The probability of a launch failure was calculated using the average failure rate of all Delta launch vehicles, or 6.5% (174 successes out of 186 attempts).

Table 6-1: Probability group definitions

Description	ID	Probability Category	Probability Value
Individual component/moving part, with heritage	1	Very Low	0.1%
Individual component/moving part, no heritage	2	Low	0.5%
Deployment - normal	3	Very Low	0.1%
Deployment - precision required	4	Low	0.5%
Scenario is completely understood and heritage systems or scenarios exist	5	Very Low	0.1%
Scenario is not completely understood, similar but not exact heritage systems or scenarios exist	6	Low	0.5%
Scenario is not completely understood, no heritage systems or scenarios exist	7	Medium	1.0%
Scenario is not completely understood, similar but not exact heritage systems or scenarios exist, lack of solution or exact heritage causes concern for design team members	8	Medium	1.0%
Technology/subsystem development, requirements are *very* strict and there exist heritage systems	9	High	5.0%
Technology/subsystem development, requirements are strict and there exist heritage systems	10	Medium	1.0%
Technology/subsystem development, requirements are *very* strict and heritage systems do not exist	11	Very High	10.0%
Technology/subsystem development, requirements are strict and heritage systems do not exist	12	High	5.0%

6.3.3 Risk Model Summary

The full TPF-I risk list and model for the *Linear DCB* architecture can be seen in Appendix A. The model consists of 101 individual failure modes or risk items. Of these, 35 result in a complete failure, 26 result in a degraded state, and 40 result in either a complete failure or a degraded state, depending on the severity or location of the failure. Almost one-third of the risk items (62) occur from a single event at a given point in time, as opposed to occurring at any point throughout the lifetime of the mission (39). A summary of the risk model can be seen in Table 6-2.

Table 6-2: Risk model summary

Total Number of Risk Items	**101**
Complete vs. Degraded State Failure	
Complete failures	35
Degraded state failures	27
Either complete or degraded state failures	39
Single Event vs. Throughout Life Timing	
Single event	62
Throughout life	39
Probability Categories	
Very high probability	1
High probability	5
Medium probability	22
Low probability	16
Very low probability	54
Unique probability	3

6.4 Results and Analysis

6.4.1 Risk Model Results

The failure modes and risk items discussed above were modeled using Matlab and the EPRA modeling approach. The star-count model discussed in Chapter 4 was used to calculate the number of stars the system could observe in both the nominal state, and all degraded states. Note that only the detection phase of the mission was modeled. Due to the use of only the detection phase, a 24 month life was assumed. A *Linear DCB* architecture was used. The minimum and maximum allowable baseline was set to 60m and 240m respectively. Finally, a single launch was assumed, resulting in 3.8m diameter apertures.

The results of the risk model are shown in Table 6-3. Given the above described architecture, TPF-I can expect to observe 116 star systems in the detection phase of the mission. Without any failures, this same architecture could observe 224 star systems. This implies that there is a 48.2% loss in observations from the risk items modeled. The current TPF-I requirement is to observe 150 star systems in the detection phase. While this number could easily change, the probability of meeting the current requirement is 46.3%.

Table 6-3: Results of TPF-I risk model

Expected Number of Observations	116.1 observations
Standard Deviation	78.4 observations
Number of Observations Without Failures	224 observations
Probability of Completing Greater than 150 Observations	46.3%
Reliability Answer	41.6%

The final value shown in Table 6-3 is the reliability answer for this architecture. If the same risk items were used to determine the reliability of the system, instead of the expected productivity, the answer would be that the system is only 41.6% reliable. This is the probability that the system is in any functioning or partially functioning state by the end of the lifetime of the mission. Providing a manager or decision maker with the option of calculating risk as expected productivity allows for the option of viewing risky missions in a more favorable light. TPF-I will be perceived as a much less risky mission if it is reported that, even accounting very conservatively for over 100 possible risk items, the mission is expected to observe over 100 stars in the detection phase. This is compared to reporting that the mission is only 41.6% reliable.

It should be noted that a pure reliability analysis can not be used to short-cut the use of a system model. The current model shows that at the end of life the TPF-I architecture is 41.6% reliable, and that without any failures the instrument could observe 224 star systems. Using only these two values, the expected number of observations would be approximated as 93.3 observations. This is a difference of 22.8 observations, or 24%, from the calculated value of 116.1 observations. This difference, shown in Equation 6-1, is due to the fact that many of the failures could occur throughout the lifetime of the mission, and that a failure at the end of life would result in a much more productive mission than a failure in the beginning of life. This example shows that a true expected productivity model, including both the probabilistic and system model aspects, is required to accurately estimate the expected productivity of a complex system.

$$\begin{aligned} E[observations]_{Estimated} &\cong Observations_{NoFailures} \times Reliability + 0 \times (1 - Reliability) \\ E[observations]_{Estimated} &\cong 224 \times 0.416 = 93.3 \\ E[observations]_{Calculated} - E[observations]_{Estimated} &= 116.1 - 93.3 = 22.8 \end{aligned} \tag{6-1}$$

Figure 6-2 shows the Cumulative Distribution Function (CDF) for the number of observations TPF-I will complete in the detection phase of the mission. The values on the x-axis are the number of observations, and the values on the y-axis are the probabilities of producing greater than each number of observations. This figure can give

the design team and science team a feel for how the probability of meeting a given requirement changes as the requirement changes. This figure also easily provides the probability of receiving no data (~21%).

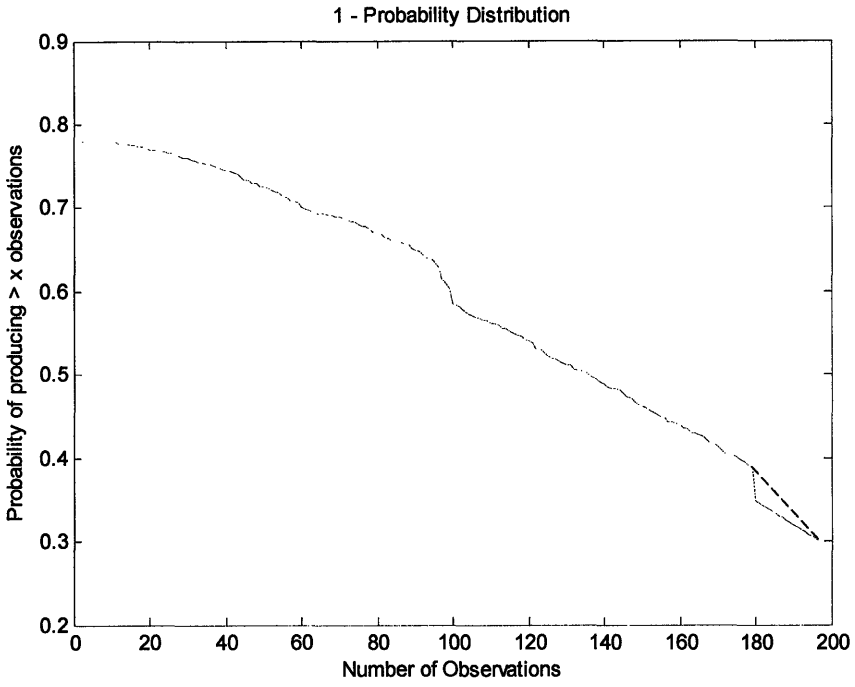


Figure 6-2: CDF of observations for TPF-I

There are two main points of interest in the shape of the CDF, as shown in Figure 6-3. There are drop-offs at approximately 100 observations and 180 observations. The drop-off in the probability of achieving greater than 180 observations is a remnant of the approximations used in the modeling process, and is not a true drop-off. As discussed in Chapter 3, the $\vec{R}$ vector is adjusted to account for situations when the system never leaves the first state. This adjustment is step 5.2 in the summary of the EPRA modeling approach (Figure 3-15) shown in Chapter 3. For the case where the system never leaves the first state, it is possible to calculate the exact time needed to observe each star system. The only cases where it is clear that the system never left the first state are cases where the last observation, or last n observations, could only be completed in the first state. In these cases either the system completed the observations still in the first state, or it did

not complete the observations at all. The probability of completing each of the observations that must be completed in the first state will therefore be lower than the probability of completing other observations. Following the expected path through the system for TPF-I, assuming both nominal and degraded states, leads to the completion of approximately 180 observations. If the system is in the first state throughout the lifetime of the mission however, it would be possible to complete 197 observations. To complete anywhere between 180 and 197 observations, this modeling approach assumes that the system would need to be in the first state throughout the lifetime of the mission, resulting in the lower probability values shown in the CDF. If all paths through the system could be mapped, this sudden drop-off would not occur, and the CDF would have a constant steep slope between the values at 180 observations and 197 observations, as shown by the dashed line in Figure 6-2 and Figure 6-3. Note that the value of 197 observations does not match the reported 224 observations with no failures. This is due to the fact that many single event failures that occur prior to operations are used to calculate the expected value of system parameters, such as observational efficiency. The difference between the expected value and the nominal value of these parameters leads to the difference between completing 224 observations with no failures, and 197 observations given the probability of these single event failures occurring, but assuming that the system did not leave the original state after operations began.

While the drop-off at 180 observations in the CDF is a remnant of the approximations used in the model, the drop-off at approximately 100 observations is real. For the TPF-I case, if the system is in a degraded three-collector state for the entire lifetime of the mission, it can only complete 102 observations. The drop-off in the CDF at this value corresponds to the adjustment in the probability matrix that changes the probabilities from the probability of being in that degraded state at that time, to the probability of being in that degraded state at that time assuming that the operations did not begin in that state. This adjustment is step 4.2.1 in the summary of the EPRA modeling approach (Figure 3-15) shown in Chapter 3. Many of the failures that could result in a three-collector system occur prior to the beginning of operations. Therefore, the fact that a three-collector system can complete only 102 observations in the given lifetime has a large impact on the CDF. If the variable phases mechanism that allows the

system to transform to a three-collector system were not included in the design, the portion of the CDF before 102 observations would essentially shift down the y-axis and meet up with the portion of the curve past 102 observations. This drop-off in the CDF is not a factor of approximations, but is a true factor of the productivity of the system, and is therefore of particular interest to engineers and designers working on TPF-I. The above explanation of the shape of the CDF curve is summarized in Figure 6-3.

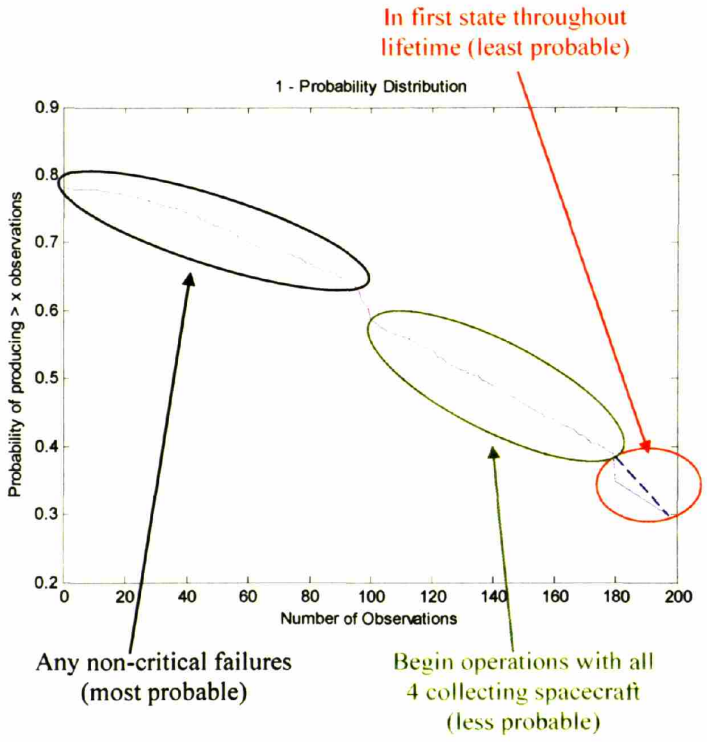


Figure 6-3: Explanation of drop-offs and shape of the CDF curve.

It is of interest to note that the drop-off that occurs at approximately 100 observations is not a sharp drop. This phenomenon is explained by the step in the analysis process where the $\vec{R}$ vector is sorted in decreasing order. This is step 5.3 in the summary of the EPRA modeling approach (Figure 3-15) shown in Chapter 3. This adjustment is done to ensure that the $\vec{R}$ vector contains the probability of completing any n observations, and not the probability of completing the first n observations in the initial star-list. In this case there are several star systems which TPF-I can complete in the first

state but not in degraded states, but which are early in the initial star-list when sorted by the time to complete the observation in the first state. When the probability of completing each observation is sorted to account for this situation, a few observations fall within the change in probabilities that occurs at the 102 observation mark, smoothing out this drop-off. This can be seen in Figure 6-4.

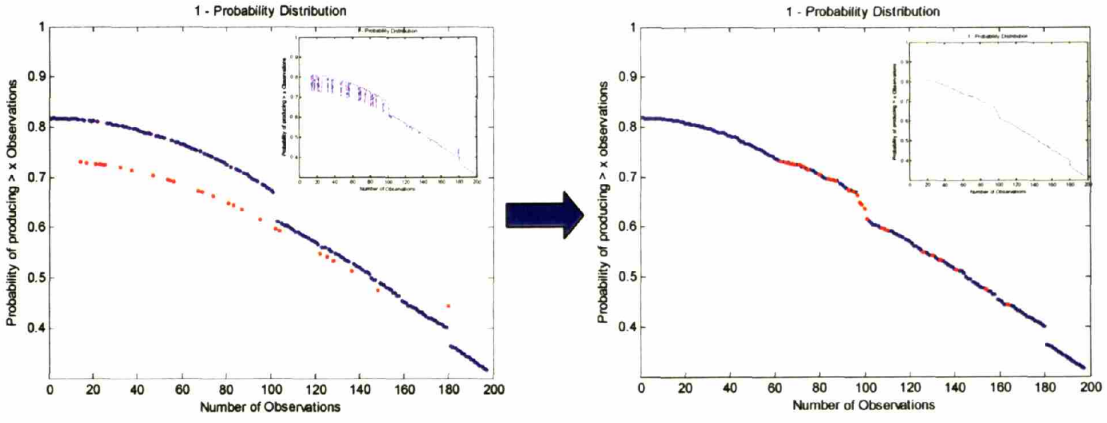


Figure 6-4: Details of the drop-off at 102 observations

6.4.1.1 Extended Lifetime Results

The results shown above assume a 24 month lifetime for the TPF-I mission, for the detection phase only. This is based on the baseline mission scenario of a 5 year life, with 2 years spent in the detection phase and 3 years spent in the spectroscopy phase. While this is the current lifetime listed in the science requirements and documents, the TPF-I design team has been instructed to carry enough consumables for an extended mission of an additional 5 years. Therefore, the same risk list was modeled using this extended life scenario, with a total lifetime of 48 months. While the total allowable time to complete observations was set at 48 months, the failure rates of failures that could occur throughout the lifetime of the mission were still based on a 24 month lifetime. This was done in order to capture the concept of designing to a 24 month lifetime, but carrying

enough consumables for a 48 month lifetime. The results of this model run are shown in Table 6-4 and Figure 6-5.

With the extra 24 month extended mission, making a total mission lifetime of 48 months, TPF-I could expect to complete 132.7 observations. This is 16.6, or 14.3%, more observations than with the lifetime set at 24 months. This increase is not as large as what may be initially expected. This is due to two factors. First, the observations are completed in order from shortest to longest completion time in the first state. Most of the star-systems for which the observations could be competed in a reasonable amount of time are already completed by the end of the 24 month lifetime. Therefore, in the extra 24 months of extended lifetime, only star-systems for which an observation would take on the order of several months are left. The second factor leading to the relatively small increase is the fact that failure rates are still determined using a 24 month lifetime. Therefore, the probability of any of these failures occurring is relatively high by the end of the 48 month lifetime, resulting in a lower expected productivity during the extended mission.

One important result of the risk model using the extended lifetime is shown in Figure 6-5. The drop-off corresponding to the number of observations that can be completed using a three-collector system moved from 102 observations to 136 observations. The extra 34 observations that can be completed if the system is in a degraded three-collector state for the entire lifetime is a very large improvement. This puts the number of observations that can be completed in one of the most severe degraded states near the required number of observations for the mission. This difference between results for the 24 and 48 month lifetimes is more significant than the difference in the overall expected number of observations of 16.

Table 6-4: Risk model results using extended lifetime of 48 months

Expected Number of Observations	132.7 observations
Standard Deviation	97.2 observations
Number of observations over Expected Observations using 24 Month Lifetime	16.6 observations
Percent Number of observations over Expected Observations using 24 Month Lifetime	14.3%

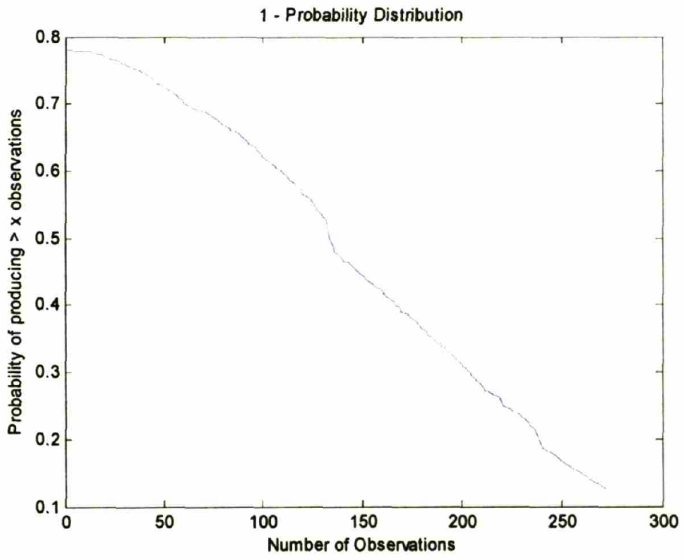


Figure 6-5: CDF of number of observations using extended lifetime of 48 months

6.4.1.2 No Technology Development Failures

As discussed previously, the risk model consists of three main categories of risks – failures of individual spacecraft, system level failures, and technology development failures. While failures of the individual spacecraft or the system as a whole are very common to include in a technical risk list, technology development failures are not as common. This is due at least partially to the fact that these failures would occur several

years before any of the other failures on the risk list would occur. Technology development is one of the first activities for a mission of this nature. If a technology development program were to fail, the results of this failure would be known for several years before the launch of the mission. This implies that the mission would either be cancelled, or designed around the particular technology development failure. Technology development failures are very important, and indeed if one design requires more technology development than another design, then the design with more technology development will be considered more risky. However, while they are important, this type of risk is usually captured separately from the technical risks of a mission. Therefore, the risk model was run again, this time without the technology development risks, for both the 24 month design lifetime and the 48 month extended lifetime. The results are shown in Table 6-5.

Table 6-5: Risk model results using no technology development risks

Lifetime	Expected Number of Observations	Standard Deviation
Design lifetime (24 months)	126.0	84.6
Extended lifetime (48 months)	144.8	105.6

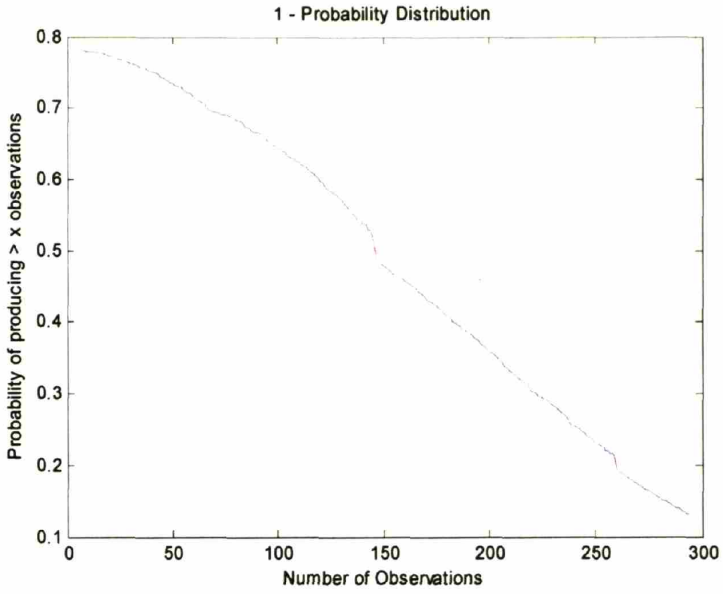


Figure 6-6: CDF for risk model using no technology development risks and extended lifetime

Without technology development risks, the TPF-I mission can expect to complete 126 observations. This is 9.9, or 8.5%, more observations than with the technology development risks included. Without technology development risks and with a 48 month lifetime, the TPF-I mission can expect to complete 144.8 observations. This is 12.1, or 9%, more observations than the 48 month case with technology development risks included. In addition, this is 28.7, or almost 25%, more observations than the case with technology development risks included, and with only a 24 month lifetime. Additionally, without technology development risks and with a 48 month lifetime, the number of observations that can be completed with a degraded three-collector system is 146. This is very near the mission requirement of 150 observations, and can be seen in the CDF shown in Figure 6-6. A comparison of all the cases discussed above is shown in Table 6-6.

Table 6-6: Summary and comparison of risk model cases

Case Definition	Expected Number of Observations
24 month lifetime, all risk items	116.1
24 month lifetime, no technology development risks	126.0
48 month lifetime, all risk items	132.7
48 month lifetime, no technology development risks	144.8
24 month lifetime, no failures or risk items	224.0

6.4.2 Mitigation and Design Change Studies

While the results discussed above are certainly informative and interesting, the absolute value of the expected number of observations for any case should be used carefully. This mistrust of numerical output, as opposed to the relative value, should be true for all risk models and analysis, since by definition the model and its inputs are uncertain. In addition, the model is only capturing the risks that have been determined by the design team. It is the relative difference between cases that is more interesting and informative. Even if the model does not capture all risks, relative values of varying case runs can determine the relative impact, and therefore importance, of those risks that are captured.

To determine the relative importance of different risk items, mitigation and design change studies were completed. These studies were carried out in a manner similar to studies to determine the Birnbaum or Fussell-Vesely importance measures, as discussed in Section 2.2. For each mitigation study, different groups of risk items were assumed to be completely mitigated, and the impact on the overall expected productivity was determined. To model a risk item being completely mitigated, the probability of

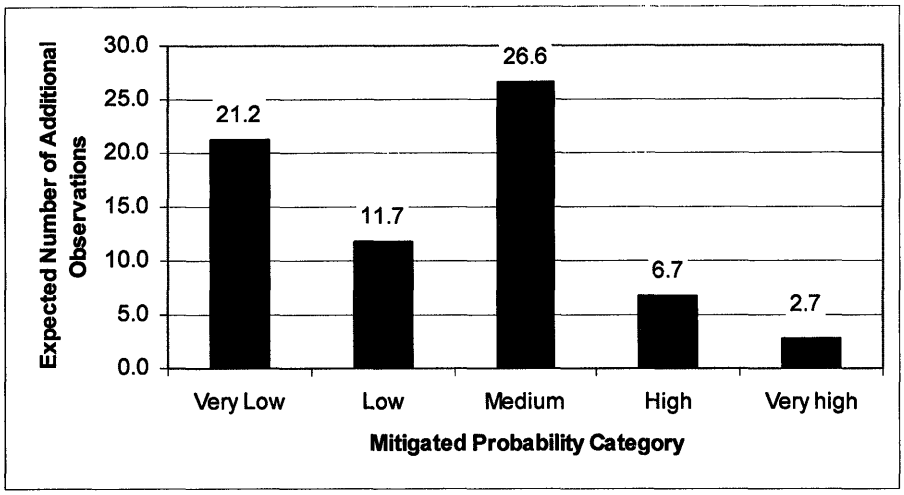
occurrence was set to zero. When the risk model was run with the probability of occurrence of a given group of risk items set to zero, the expected number of observations increased with respect to the case where no risk items were mitigated. The amount of this increase indicates the level of importance of that particular group of risk items. The same concept was used in design change studies. Instead of mitigating a group of risk items, one particular aspect of the design was changed. An example of a design change would be to remove a level of redundancy. In this case, the number of expected observations decreased from the expected number of observations for the case without the design change. In the same manner as the mitigation studies, the difference between the expected productivity, with and without the design change, indicates the level of importance, in terms of risk, of that aspect of the design.

6.4.2.1 Probability Category Mitigation Study

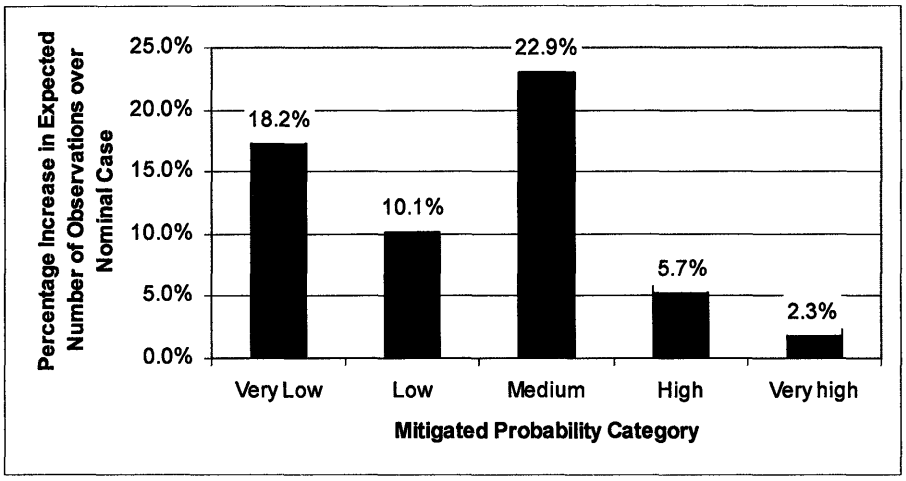
The first mitigation study that was completed was a study comparing the importance of all the risk items in each of the five probability categories. The results of this study can be seen in Figure 6-7.

Medium and very low probability risk items have the highest impact on the total expected productivity of this system. This is not unexpected. The majority of risk items (54 out of 101) are very low probability. The second largest number of any one probability category is medium probability risks (22 out of 101). While there is more than double the number of very low probability risks than there are medium probability risks, the medium probability risk items still have the highest impact on the overall system expected productivity. This is because while there are a very large number of very low probability risk items, each individual item has by definition a very low probability of occurrence. The higher probability of occurrence for the medium probability risk items leads to a larger impact when mitigated. While the very low probability risk items have only a small impact individually, there are enough of these risk items that mitigating all of them still has a very large impact on the overall system productivity. Note that even though by definition they have the highest probability of

occurrence, the small number of high (5 out of 101) and very high (1 out of 101) probability risk items leads to a very small impact on the expected productivity of the system if they are mitigated. In addition to the small number of risk items that fall into these categories, those risk items that have high or very high probabilities of occurrence are also all technology development risks. All technology development risks are degraded state risks, and therefore have smaller impacts than the risks that lead to complete failure.



a. Expected Number of Additional Observations

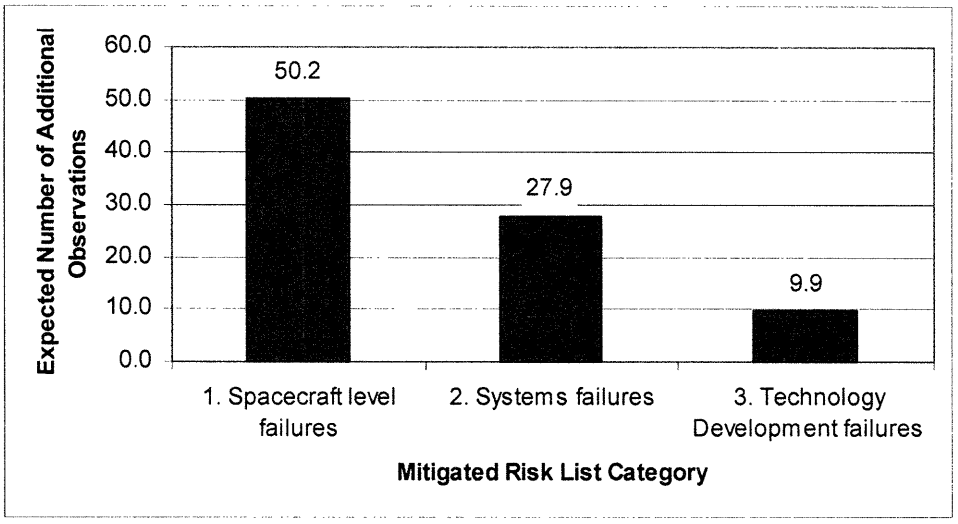


b. Expected Percentage of Additional Observations

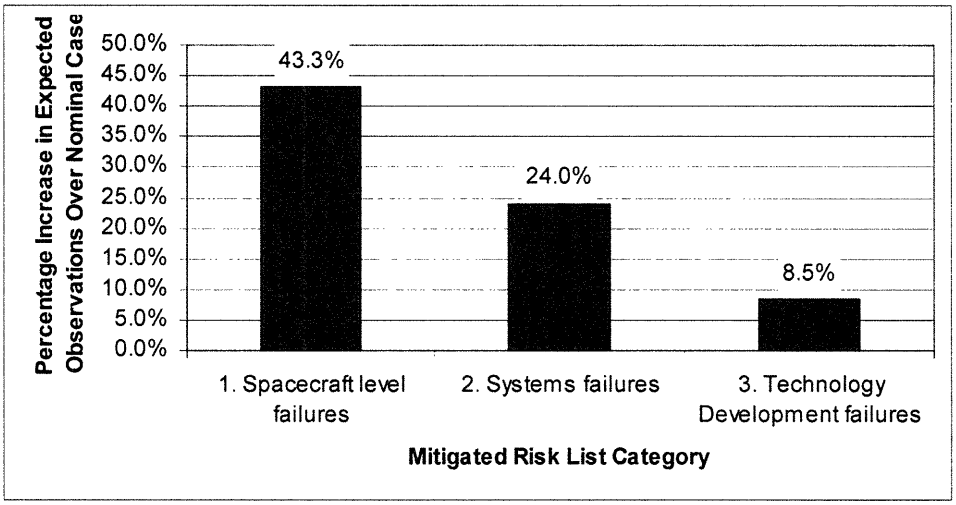
Figure 6-7: Results of the probability category mitigation study

6.4.2.2 Risk List Category Mitigation Study

The second mitigation study compared the importance of the risk items in each of the various risk list categories. The results from this study can be seen in Figure 6-8.



a. Expected Number of Additional Observations



b. Expected Percentage of Additional Observations

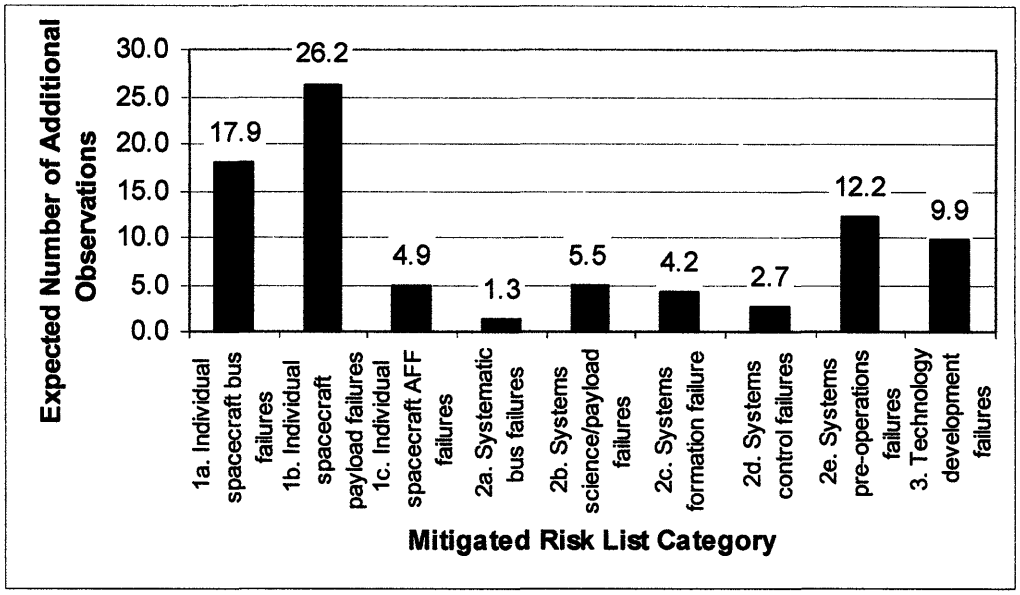
Figure 6-8: Results of the risk list category mitigation study

The difference in the importance level of the three main risk list categories is quite dramatic. Of the 101 risk items modeled, 50 are spacecraft level risks, 41 are system level risks, and 10 are technology development risks. The technology

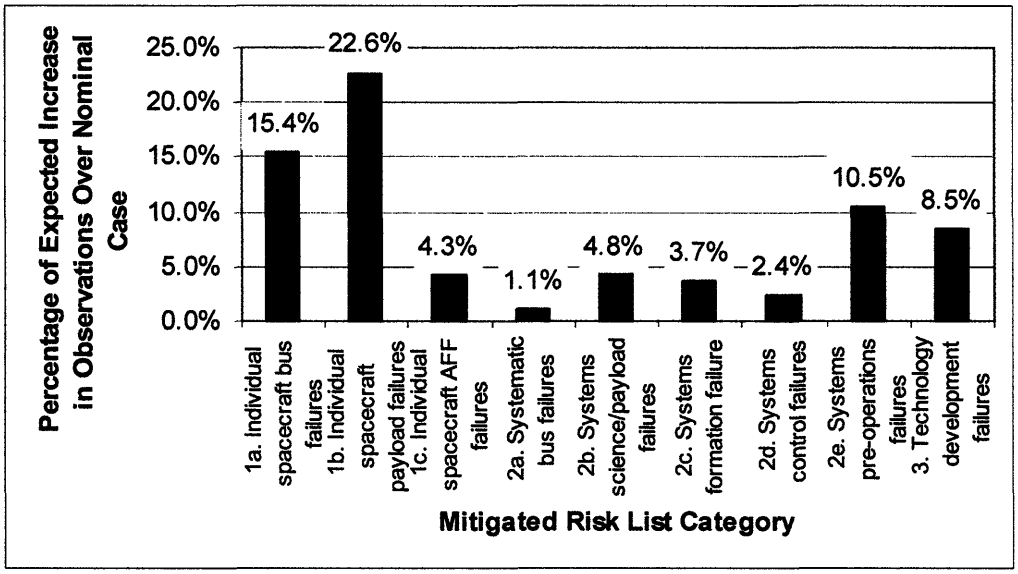
development failures have the lowest impact on the overall expected productivity of the system by a large margin. This is not unexpected since there are many fewer risk items that fall into this category compared to the other categories. In addition, all technology development risks are degraded state risks, making the impact of this category less than the impact of either category that contain complete failure risks.

Spacecraft level risks impact the overall expected performance of the TPF-I mission much more than system level risks. In fact, removing the spacecraft level risks from the system would increase the expected productivity by almost twice as much as removing the system level risks. This is due in small part to the fact that there are more spacecraft level risks modeled than there are system level risks. The difference in the number of each type of risk item is relatively small however, at only 9 additional risk items in the spacecraft category. The main difference between these two categories is that most risks in the spacecraft level category are repeated on 5 different spacecraft. As an example, any aerospace mission will require an ACS subsystem. TPF-I, however, requires 5 separate ACS subsystems. A failure in any one of these subsystems affects the mission productivity, and a single failure in any one of three of the ACS subsystems would result in complete mission failure. This system of systems nature of the TPF-I mission means that any relatively minor and normal risk that other aerospace systems might face is multiplied in importance for this mission.

An additional mitigation study was carried out to determine the importance of each of the subdivided risk list categories. The results are shown in Figure 6-9, where it is seen that the individual spacecraft payload failures have the largest impact on overall expected productivity. Each payload, on each spacecraft, requires a very large number of precision moving parts. The failure of a single actuator on a single fast-steering mirror could lead to mission failure. For these components there is no method of adding redundancy, without adding an entirely redundant optical path. Reducing the number of single point failures on each individual spacecraft payload would make a very large difference in the expected productivity of the mission.



a. Expected Number of Additional Observations



b. Expected Percentage of Additional Observations

Figure 6-9: Results of the detailed risk list category mitigation study

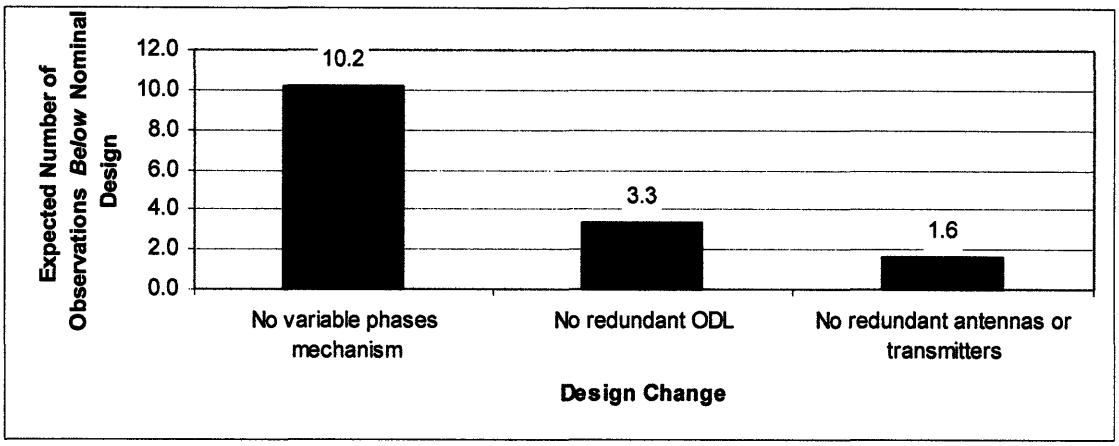
The individual spacecraft bus failures also have a relatively large impact on the expected productivity for TPF-I. This result is more unexpected than the result of payload failures having a large impact. Two of the major perceived risks for the TPF-I mission are the number of single point failure moving optical elements, and the formation

flight system. The results of the model show that the "every-day" engineering functions are nearly as important, in terms of risk, as the optical elements, and are significantly more important than the formation flight system. This is an especially important result with the realization that the risk list was put together with a focus on unique failure modes, mostly dealing with the instrument and formation flight system. This implies that the importance of the bus failures, or engineering functions, may be even larger than shown in Figure 6-9. The result that, in terms of risk, these engineering functions are very important to TPF-I, is both a major and unexpected result.

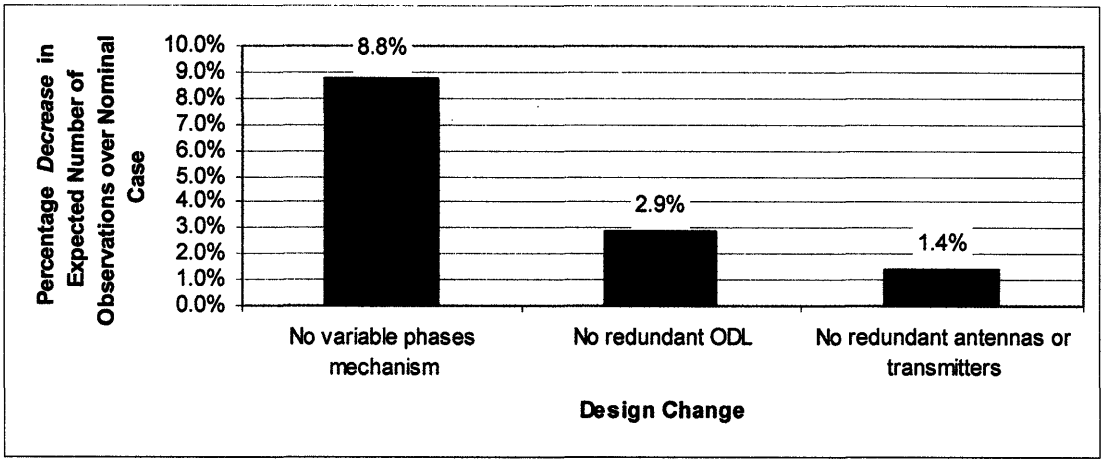
Of system level failures, the only category that has a significant impact on the overall expected productivity of the system is the pre-operational failures. Pre-operational failures have a larger impact on expected productivity than failures that occur throughout life, because if a pre-operational failure occurs the mission will produce zero return. In contrast, a failure that can occur throughout life has a possibility of occurring at the end of life, resulting in a relatively productive mission.

6.4.2.3 Design Change Study

A design change study was carried out to determine the effect of three different design changes on the expected productivity of the mission. The current design includes some redundancy for both the optical delay lines and the AFF antennas and transmitters. Both of these layers of redundancy were removed to examine the impact. The current design also calls for a mechanism to allow for variable phases in the beam combiner. This mechanism allows for the possibility of having degraded three-collector systems, but also introduces the risk of the mechanism failing in the degraded state mode. This mechanism was also removed from the design to examine the impact on the overall expected productivity. The results of this study are shown in Figure 6-10.



a. Expected Decrease in Observations



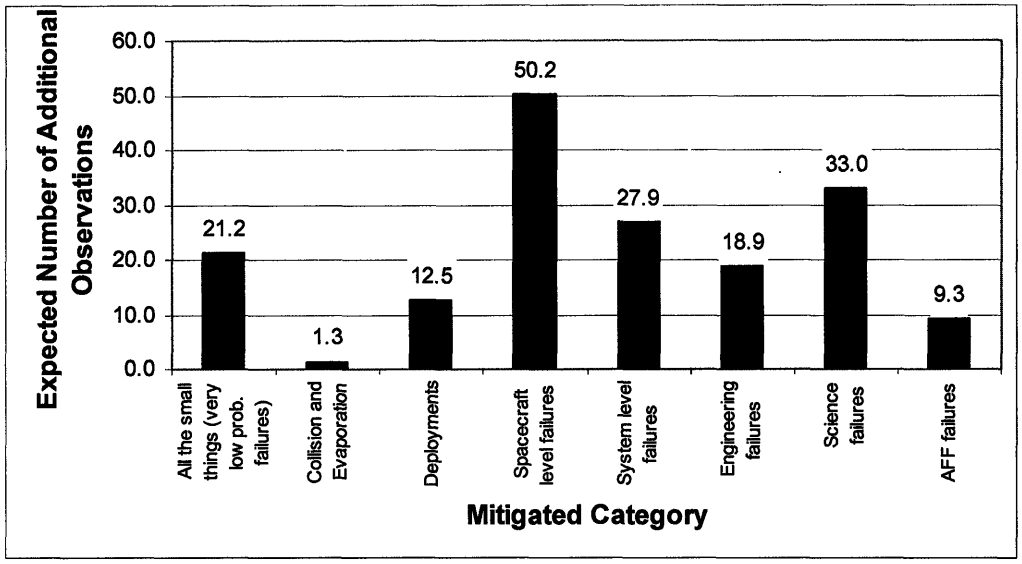
b. Expected Percentage Decrease in Observations

Figure 6-10: Results of the design change study

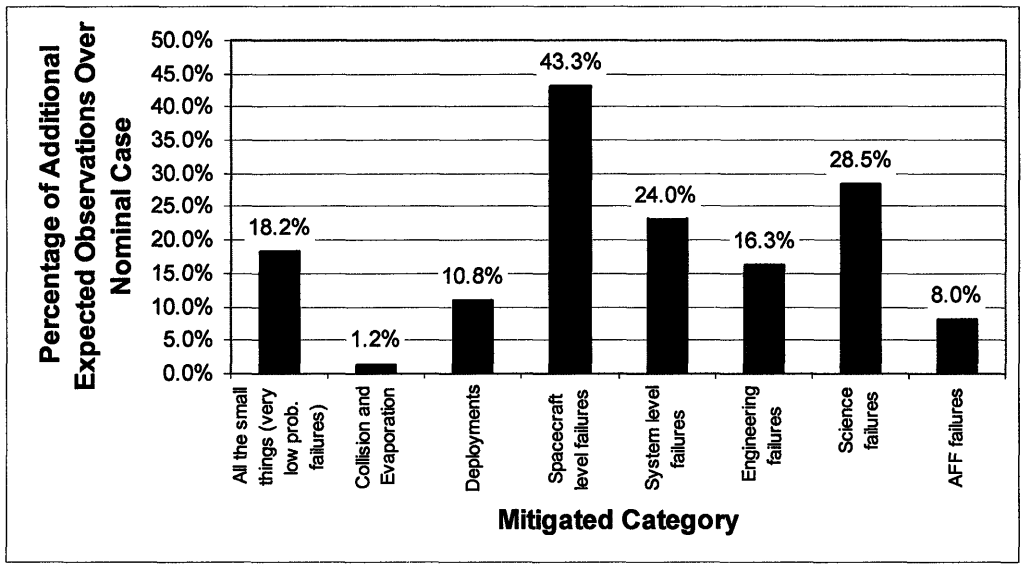
Redundancy, both in the optical delay lines and the AFF system, does not lead to a significant increase in the expected productivity of the overall system. It should be noted that the AFF antennas and transmitters may have a more complicated redundancy scheme than is modeled, leading to a larger impact on the expected productivity. The variable phases mechanism does have a significant impact on the expected productivity of the TPF-I mission. Including the ability to vary the phases of the beams leads to 10.2 more expected observations than if this ability were not included.

6.4.2.4 Major Perceived Risk Areas

In addition to the individual studies discussed above, the importance of all areas of the TPF-I design that are often perceived to be risky were compared, in terms of expected productivity. The results of this study can be seen in Figure 6-11.



a. Expected Number of Additional Observations



b. Expected Percentage of Additional Observations

Figure 6-11: Results of the major perceived risk items mitigation study

Spacecraft level failures have the largest impact on the expected productivity. As discussed above, this is due to the fact that many of these risks are multiplied by five spacecraft. Comparatively, system level failures have almost half the impact of these spacecraft level failures. A separate study, to examine in depth the most efficient way of improving the reliability of each of the individual spacecraft, could lead to a very large positive impact on the expected productivity of the TPF-I mission.

One of the concerns that is mentioned most often when discussing the risks associated with TPF-I is all the small things that are required to work for the system to work. This concern is modeled by mitigating all very low probability failures. As mentioned above, there are many single point failures in this mission, including many moving optical elements. While each of the failures in this category has a very low probability of occurrence, the number of failures increases the impact on the system as a whole.

Collision and evaporation are viewed by many managers as two of the most major risks for TPF-I. In the current model, collision and evaporation are both medium probability, complete failure risk items. In addition, many other failure modes lead to an increase in the probability of collision and evaporation. Completely mitigating these two failure modes still leads to an expected increase of only 1.3 observations, or 1.2%. While these risk items are perceived by many to be some of the most major risks TPF-I faces, in reality they have relatively little impact on the expected productivity of the mission.

TPF-I has an especially large number of deployments. Each of the five spacecraft needs to deploy the sunshades, stray-light baffles, cryo-radiators, and solar arrays. Additionally, the combining spacecraft needs to deploy the high-gain antenna, and each collecting spacecraft needs to do a precision deployment of the secondary mirror. Most of these deployments are also complete failure risks, and all occur prior to the beginning of operations. Therefore, it is not surprising that the deployments for TPF-I have a significant impact on the expected productivity.

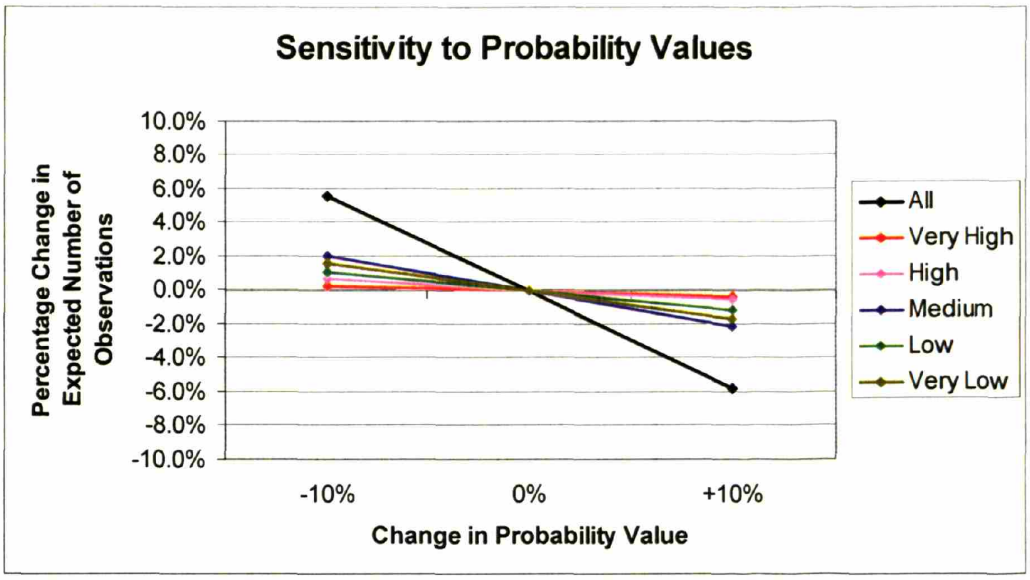
The final thing to note about Figure 6-11 is the relative impact between the engineering, science, and formation functions. The science functions have the largest

impact. This is not surprising due to the complexity of the interferometer functions. The engineering functions also have a relatively large impact on the expected productivity. In fact, the engineering functions have more than half the impact of the science functions, and are significantly more important than the formation functions. As discussed previously, the result that, in terms of risk, these engineering functions are very important to TPF-I, is both a major and unexpected result.

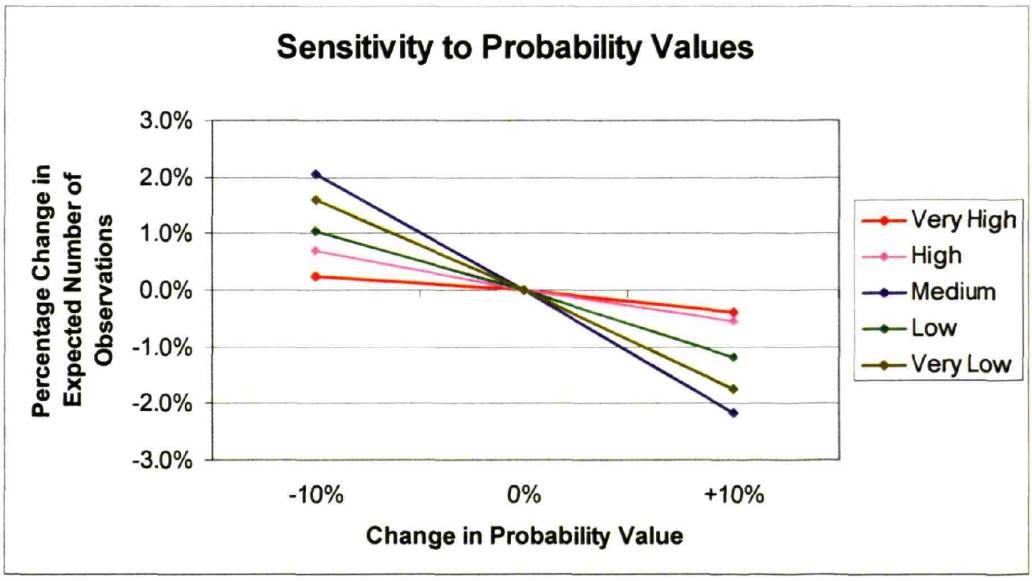
6.4.3 Sensitivity Studies

As discussed above, the output of any risk model will by definition be uncertain. Probability values are based on engineering judgment alone and can very rarely be verified. While the impact of some failures can be modeled with significant certainty, such as the productivity of a system with one fewer spacecraft, the impact of other degraded state failures is very uncertain. This is especially true if the impact of the failure results in the change of a system level parameter, such as observational efficiency or the failure rate of a different failure mode. Therefore, sensitivity studies were carried out to determine the sensitivity of the expected productivity modeling results presented above to the specific probability values assigned to each probability bin, as well as to the level of impact of failures on system parameters.

The first sensitivity study was conducted to determine the sensitivity of the expected number of observations to the specific values assigned to each probability category. Each probability value was adjusted by ±10% individually. Additionally, all probability values at once were adjusted by ±10%. The results are shown in Figure 6-12.



a. All results



b. Results of individual probability bins only

Figure 6-12: Results of probability value sensitivity study

Even in the most extreme case, when all probability values were adjusted by ±10% at the same time, the resulting expected number of observations still varied by less than 6%. If a single probability value is incorrect, the effect was even more minimal. The expected productivity results were most sensitive to the probability value assigned to

the medium probability risk items. Even in this most sensitive case however, the change in the expected observations, for a 10% change in the probability value, was only approximately 2%.

The second sensitivity study examined the sensitivity of the expected productivity results to the uncertain degraded state productivities. In several cases a degraded state productivity was calculated by adjusting one or more system parameters. These system parameters included observational efficiency, probability of collision and evaporation, lifetime, integration time, minimum baseline length, and maximum baseline length. The most common parameters affected by other failure modes were observational efficiency and the probability of collision and evaporation. The factor by which each parameter is impacted varies from failure mode to failure mode. The most common impact of failures is to alter system parameters by a factor of either two or five. Therefore, this study examined the sensitivity of the expected productivity results when all factors affecting the probability of collision and evaporation were set to five, when all factors affecting the observational efficiency were set to two, and when all factors affecting any of the system parameters were set to two. The results are shown in Table 6-7.

Table 6-7: Results of impact sensitivity study

Description	Expected Number of Observations	% Difference from Baseline Case
All impacts affecting Collision and Evaporation changed to x5	116.1	-0.02%
All impacts affecting Observational Efficiency changed to /2	116.5	0.34%
All impacts changed to x2 or /2	117.0	0.76%

Alterations to the factors applied to system parameters used to adjust the productivity in degraded states made very little difference on the total expected productivity. Changes to the factors affecting a single system parameter affected the

results of the risk model by less than 0.5%. Even when the factors affecting all system parameters were adjusted, the result still varied from the baseline case by less than 1%. This insensitivity to the specific factors applied to system parameters to adjust the productivity of degraded states removes a large amount of uncertainty in the results of the TPF-I risk model.

6.5 Conclusions and Recommendations

The main conclusion to the TPF-I risk model and analysis is that the TPF-I mission is not as risky as originally perceived. In all cases examined, over 100 observations can be expected to be completed. In addition, when using the slightly less conservative, although still realistic inputs of an extended 48 month mission lifetime and no technology development failures, the expected number of observations is 144.8. This is very close to meeting the mission requirement of 150 observations, which is set without any consideration of risk or failures. It has also been shown that while these numbers should still be used carefully in an absolute sense, the outputs of the model are not sensitive to the two most uncertain inputs – the probability values used and the unknown productivity of certain degraded states.

The mitigation and design change study results led to several recommendations of future directions for the TPF-I mission. First, a detailed study should be conducted to determine the best way to improve the reliability of the individual spacecraft. This study should examine the best places to add redundancy, or to increase testing, to ensure a lower probability of failure of the individual spacecraft. It is very important to keep in mind that any study of this nature should not ignore the "every-day" engineering functions of the spacecraft, as these may have a very large impact on the overall expected productivity of the TPF-I system as a whole. The best course of action for TPF-I as a project may be to improve the reliability of components and functions that are not unique to TPF-I, but are used on many aerospace missions.

Design improvements that would have a large impact on the expected productivity of the TPF-I system include decreasing the number of required deployments,

and ensuring that the ability to include variable phases remains in the design. Each of these design improvements would result in a direct increase of over 10 expected observations.

Finally, all risk items categorized as medium probability should be examined in detail. These risk items should be examined to ensure that they truly are medium probability, and to determine if there is anything that can be done to reduce this probability. Not only do these risks have a large impact on the overall expected productivity of the system, but they will also be easier to improve, in terms of probability of occurrence, than a risk item that currently has a low or very low probability.

Chapter 7

Conclusions

7.1 Thesis Summary

Risk is clearly viewed as an important design parameter throughout the aerospace industry. However, risk is not used to the extent it could be when making design decisions. This is especially true for design decisions made in the early conceptual design phases.

The risk analysis and modeling approaches that are currently used in the aerospace industry date back to their heritage with human spaceflight and the nuclear industry. This heritage has led to all aerospace systems being treated as safety-critical systems from a risk perspective. If a system is safety-critical, then any critical failure has the same consequence – loss of human life. This consequence is so large that the consequence of any non-critical failure can be considered negligible. In non-safety critical systems however, the consequence of failures may vary drastically. This is due both to the consideration of non-critical failures, such as degraded state failures, and to the factor of when a critical failure occurs. If a critical failure occurs early in the lifetime of a mission, the impact on the scientific return of the mission will be much greater than if the same failure had occurred towards the end of the lifetime of the mission. This difference between the impacts of failures depending on when the failure occurs is ignored using current aerospace industry risk assessment techniques.

The definition of risk is the combination of the probability of a negative event occurring and the impact of that event. Therefore, the current risk assessment techniques used in the aerospace industry are actually reliability analyses, and not risk analyses, since the previously discussed varying impacts are not considered for non-safety critical

systems. To complete an accurate risk assessment, it is important to bring together the fields of system performance and reliability, to accurately model the expected value of the total system productivity, accounting for the possibility of failures throughout time. This type of analysis is called expected productivity analysis.

Examples of the productivity metric of missions include the number of star systems observed, the number of rocks sampled, or the distance traversed. While the metric will vary between missions, it will always represent the return, or productivity, of the mission. Therefore, the expected value of the productivity metric will always be a parameter that is well understood by the designers and engineers on a team. Expected productivity analysis is a good risk assessment technique because it is quantitative, and calculated at the same maturity level as productivity modeling. When expressed quantitatively, risk can be incorporated as a factor in design decisions and trade space analyses. Additionally, since expected productivity can be calculated at any fidelity level that the mission productivity model is calculated at, it can be used at any point in the design life-cycle. Expected productivity analysis also has the capability to model and take into account the productivity of potentially important degraded states. Most importantly, expected productivity analysis captures the varying impacts associated with when a failure occurs.

An example was given in Chapter 2 to illustrate the importance of the varying impact of failures based on timing. In this example a very simple system was analyzed using two risk analysis techniques – one that uses probability of failure as the risk metric, and the other that uses expected productivity as the risk metric. Two failure modes were modeled. The first failure mode involved a deployment failure, which would occur at a single point in time prior to operations. The second failure mode involved the failure of a moving component, and it was assumed that this failure could occur at any point throughout the lifetime of the mission. The two analysis approaches were used to determine the more important risk, between the deployment failure and the failure of the moving component. It was shown that the two approaches often provided opposite answers. This example showed that risk analysis techniques that use the probability of failure by the end of the mission lifetime as the risk metric may not correctly identify the

most important risk items, in terms of both probability and impact, and could therefore lead to improper risk mitigation investment decisions.

While an expected productivity analysis is relatively simple to complete if the productivity of the system depends only on the functional state of the system, the required calculations become much more complex if the productivity of the system is path-dependant. An example of a system with a path-dependant productivity function is an observatory. The time required to observe a given star system may depend not only on the functional state of the observatory, but also on the stellar characteristics, such as luminosity and distance. The same path-dependant productivity situation is true for nearly all space missions. The time required for a rover to traverse a given distance will depend on the characteristics of the terrain, and the time required to send a transmission will depend on the size and complexity of the data. For systems with path-dependant productivity functions, the productivity in each state depends on which action in a list of actions the system is executing at that time, which, in turn, depends on the amount of time the previous actions took, and therefore depends on the previous states of the system. The system itself is still a Markov system, since the current state of the system depends only on the previous state. The productivity however, is now time and path-dependent, making the calculation of the expected productivity much more complicated. While Monte Carlo simulations can capture this effect, these simulations take a long time to run and are very inefficient, especially when utilizing complicated performance functions. This inefficiency is particularly harmful when broad architecture trade-spaces are being explored, and the number of systems to be analyzed is very large. A more time and effort saving approach to modeling the overall expected productivity of systems with path-dependent productivities could improve both the accuracy and efficiency of these modeling efforts.

An approach has been developed to model the expected productivity of systems with path-dependant productivities in a more efficient and effort saving manner than a Monte Carlo simulation. The approach is called Expected Productivity Risk Analysis (EPRA). The basic principle behind the EPRA approach is to find the expected path, and then find the expected productivity given the expected path. Initial conditions are set by

failure modes that occur prior to the beginning of operations. The probability of being in each state throughout time is then found using Markov modeling, and the number of time steps required to complete each object is determined using a productivity model. An object is defined as a single unit of the performance metric, such as an image or a measurement. Next, the expected number of time steps to complete each object is found. Based on these expected times to complete each object, the probability of being in any functioning state at the end of each number of objects is calculated. Finally, the probability of completing exactly each number of objects, and therefore the expected number of objects completed, the standard deviation, and the Cumulative Distribution Function (CDF) are calculated.

The EPRA approach has been tested against a Monte Carlo simulation with excellent results in terms of both accuracy and speed. When tested using 35 various scenarios, the EPRA approach produced results that varied from the Monte Carlo results by an average of less than a quarter of one percent, while completing the calculations up to almost 275 times faster. In addition to matching in terms of the overall expected productivity results, the EPRA approach results also matched the Monte Carlo results in terms of the CDF for the productivity, as shown in Figure 7-1.

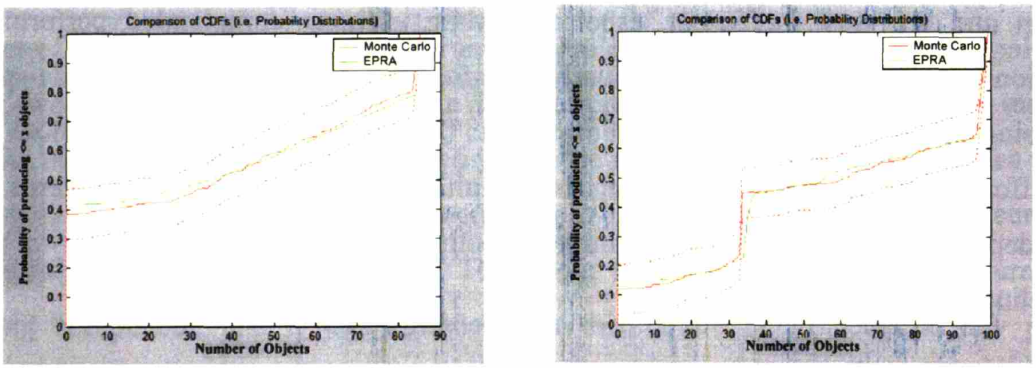


Figure 7-1: CDFs for two different tested scenarios. The solid green lines show the new EPRA path-dependant simulation results while the red lines show the Monte Carlo results (dashed lines represent the 95% confidence interval)

Examples presented in this thesis have shown expected productivity both can, and has impacted a design, through two case studies using a real mission, Terrestrial Planet Finder Interferometer (TPF-I). TPF-I is an interferometer mission, consisting of multiple individual spacecraft flown in formation. The first case study discussed in this thesis identified and analyzed the major degraded states for various TPF-I architectures. For this study, spacecraft level failures only were considered. The various candidate architectures for TPF-I were compared in terms of the performance of the remaining system, given a failure of an individual spacecraft. The ability to perform in the event of a major failure is known as graceful degradation. This study examined both the ability of each of the architectures to degrade gracefully, as well as possible design changes to achieve more graceful degradation.

The graceful degradation case-study had two major results. First, a design decision to switch the type of beam combiner instrument used on TPF-I was recommended based on the results of this study. The study showed that, without the ability to vary the phases of the beams from the collectors, no architectures could support any interferometric capabilities after the loss of a single spacecraft,. With the ability to vary beam phases however, multiple architectures, including the front-running *X-array* and *Linear DCB*, could have productive degraded states without certain spacecraft in the array. While the beam combiner design that was being pursued does not support variable phases, a previously considered beam combiner design *could* support this capability. Therefore, a recommendation was made by the instrument design team lead to switch the design of the beam combiner instrument, to include this ability to vary the phases of the incoming beams and allow for graceful degradation. Because this study was completed at such an early point in the design process this decision to switch designs, to a design that is inherently more robust to failures, was possible.

The second major result from the graceful degradation case-study was an input to, and effect on, the architecture trade study and down-select for TPF-I. The various candidate architectures for TPF-I were judged based on 27 different parameters, including the ability to degrade gracefully. Each parameter was given an importance weighting, with the sum of all weightings equaling 100. This led to a average weight of

3.7 per parameter. Graceful degradation was given an above average weighting of 4.3. This led to the graceful degradation parameter having a significant impact on the outcome of the architecture trade-study. As an example, the point difference between the *Linear DCB* and the *Diamond* architectures was 20 points, while the total point difference between these two architectures was only 31 points. By introducing risk analysis at an early phase in the design, through expected productivity, it was possible to make risk a direct factor in a major architecture decision.

The other major case-study discussed in this thesis identified and analyzed the major risks to the front-running TPF-I architecture, the *Linear DCB* architecture. Design team members and experts were interviewed to identify the risks associated with the mission. This led to a risk list with 101 risk items. These risk items were then modeled, using the new EPRA approach. The TPF-I star-count model, that was developed by the TPF-I team for performance trades, was used as the productivity model. The results of this modeling effort showed that TPF-I can expect to complete 116 observations in the detection phase of the mission. In addition to the expected number of observations, a CDF was produced to show engineers and designers the probability of completing greater than any given number of observations. The CDF for the nominal TPF-I design is shown in Figure 7-2.

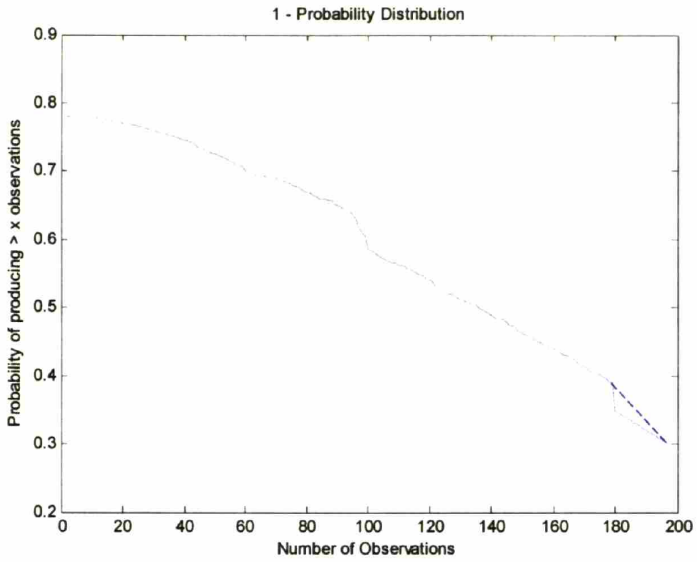


Figure 7-2: CDF results of TPF-I risk model

To determine which risk items have the largest impact on the overall system risk, mitigation and design change studies were completed. In these studies, the risk model was run with categories of risk items mitigated, modeled by setting the probability of occurrence to zero. The effect of the risk items was then determined by comparing the expected number of observations with and without the mitigations. An example of the results of these mitigation studies is shown in Figure 7-3. Results of the mitigation and design change studies led to several recommendations for future work regarding risk mitigation for TPF-I. These included a detailed study to examine how best to improve the reliability of the individual spacecraft in the array, reducing the number of deployments required, and examining in detail mitigation options for all of the risk items categorized as medium probability.

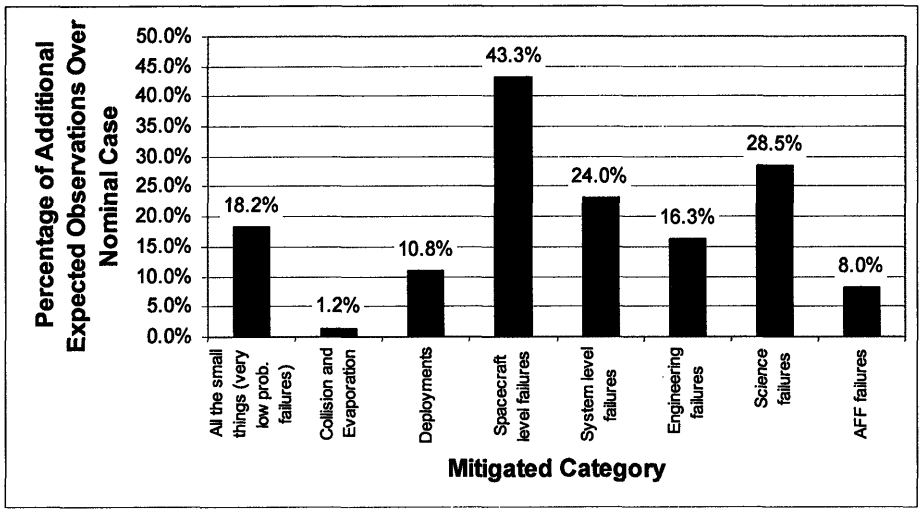


Figure 7-3: Example of mitigation study results for TPF-I risk model

The work presented in this thesis has suggested that the expected value of the performance metric of the system, defined as the expected productivity, is a very valuable metric to represent the technical risk level of a mission. It has been shown that using the probability of failure by the end of lifetime as a risk metric does not appropriately capture both aspects of risk for non-safety critical systems, since the varying impacts of failures at different points in time throughout the mission is not accounted for. The work presented in this thesis has presented expected productivity analysis as a new risk analysis technique. This technique has been implemented on a JPL pre-formulation flight mission, TPF-I, and has had an impact on design and architecture decisions. By using this new technique for risk analysis, that can be implemented in the pre-formulation phases of a mission and can truly capture all aspects of risk, it will be possible to use risk analysis results to impact design decisions at an early phase of the design process. This will reduce the cost of risk-mitigating decisions, and will make future missions both lower risk and less expensive.

7.2 Contributions

This thesis has developed a new approach for risk analysis using expected productivity. A new modeling approach for determining the expected productivity of systems with path-dependant productivities was developed and tested. Finally, the approach of using expected productivity as a risk analysis methodology was demonstrated using two case-studies from a JPL mission, TPF-I. The specific contributions of this research are as follows:

1. Introduced the concept of using expected productivity as a complete risk analysis technique for non safety-critical systems. Expected productivity analysis models all components of the risks to a mission, including both the likelihood and impact, in a quantitative way that can be applied at any stage in the design process.

    1.1. Developed the rationale for why to use expected productivity as a risk metric. This rationale was developed by first showing why current, probability of failure based, techniques do not capture risk in an appropriate way for non-safety critical missions. The rationale for why expected productivity covers the holes of probability of failure based techniques, and therefore makes a more appropriate risk metric for non-safety critical systems, was then developed.

    1.2. Developed a new importance measure for use with expected productivity analysis. This new importance measure was then compared to existing risk importance measures, using a simplified example.

2. Developed a new modeling approach, EPRA, which estimates the expected productivity of systems with path-dependant productivities. The EPRA approach can be applied to a large number of aerospace systems that have path-dependant productivities, including but not limited to, observatories or rovers.

2.1. Documented the mathematical approach in a step-by-step manner. This should allow for simpler implementation on new missions or projects.

2.2. Tested the new EPRA approach against the only existing approach, Monte Carlo simulations. The EPRA approach results had very good accuracy, with much shorter calculation times, when compared to the Monte Carlo simulations.

3. Provided examples of how risk analysis in conceptual design can be used to affect design decisions early in the design process, using a JPL pre-formulation phase flight mission, TPF-I.

3.1. Initiated a suggested design change to the TPF-I mission. The work presented in this thesis led the instrument design team lead for the TPF-I mission to suggest a design change. This design change will significantly reduce the risk to the TPF-I mission, while not significantly increasing the cost of the mission, since the change will be made at such an early point in the design cycle.

3.2. Completed the TPF-I graceful degradation case-study. Rules for operating in a degraded state were developed, and used to determine the productivity in degraded states for all candidate architectures. Design changes that would improve the graceful degradation capabilities of each of the architectures were also identified. Finally, input was provided to the architecture down-select and trade study, on the level of graceful degradation of each of the candidate architectures, in terms of both productivity in the degraded states and likelihood of reaching a degraded state. This led to risk being used as a direct factor in a major architecture decision for TPF-I.

3.3. Completed a risk list, model, and analysis for the TPF-I design team. Gathered a list of major risks to the TPF-I mission through expert

interviews. Modeled the risk items using the EPRA modeling approach. Provided analysis results, including nominal results, mitigation study results, and design change study results, to the TPF-I design team. Made several recommendations for risk mitigation to the team, based on the study results. Specific recommendations include completing a follow-on study to examine how best to improve the reliability of individual spacecraft, and examining in depth all risk items labeled with a medium probability of occurrence.

7.3 Recommendations for Future Work

While the work presented in this thesis takes a large stride towards improving risk analysis techniques for use with missions in the early design phases, there are certainly many related areas of exploration that should be studied in the future. Specific areas recommended for future study include:

- Develop a more efficient software tool to implement the EPRA approach.
    - The current implementation of the EPRA approach can take anywhere from several minutes to several hours to complete a single analysis, depending on the complexity of the productivity model used. While this is certainly much more efficient than running a Monte Carlo simulation, it can still be hampering to run for very large trade space analyses. Therefore, developing a software tool that can implement the mathematical approach presented in this thesis in a more efficient manner would be very useful.
    - Determine a more appropriate software environment, and implement the EPRA approach in that environment. The work presented in this thesis was implemented using Matlab. While this software environment worked for the case-studies presented in this

thesis, it is limited in its memory availability, and can accommodate limited sizes of matrices. Determining a software environment that could accommodate the memory and matrix sizes required to complete studies larger than those presented in this thesis, and implementing EPRA in that environment, could be very useful in the future.

- Additional case studies to show how expected productivity can be used as a risk analysis tool.
    - In order to be proven as a risk analysis methodology that will work on all classes of missions, expected productivity analysis needs to be implemented on case-studies that do not involve observatory missions. Examples include completing an expected productivity analysis of a Mars rover or orbiter, or a Lunar rover or orbiter.
    - One of the main recommendations resulting from the risk analysis for TPF-I is to complete an additional risk analysis study on the individual spacecraft in the TPF-I array. This study should include all science and engineering functions on the individual spacecraft.
    - There are many areas where redundancy could be built into the TPF-I design. These include redundant components, such as sensors, a fully redundant optical train, or a fully redundant spacecraft. A study to determine where the best areas to add redundancy to the TPF-I system, in terms of expected productivity, could be very useful.
    - One of the main considerations for risk mitigation for the TPF-I mission is to fly a spare spacecraft. However, all of the architectures under consideration have multiple types of spacecraft in the array. A study to determine which type of spacecraft has the largest impact if flown as a spare, in addition to whether or not it is

worth designing a spare spacecraft that could work as a spare for multiple types of spacecraft, could be very helpful to the TPF-I mission.

- Determine the most appropriate way to integrate existing reliability-based tools into the expected productivity analysis methodology. Reliability-based tools and methodologies have sophisticated capabilities to identify risks, as well as to calculate probabilities of occurrence throughout the lifetime of the mission. Examples include quantitative fault tree and phased mission system analysis tools. Combining one or more of these reliability-based tools with the expected productivity analysis methodology presented in this thesis could lead to a very powerful risk assessment tool suite.

- Apply various probability distributions to the EPRA approach. The work presented in this thesis assumed an exponential failure rate for all failures that could occur throughout the lifetime of the mission. It would be interesting to study the effect of other failure rate distributions, including Bathtub curves and Weibull distributions, on expected productivity analysis results.

- Develop a methodology for analytically calculating the uncertainty bands on EPRA results, to determine confidence intervals and sensitivity analyses. This would require a new methodology for analytically propagating uncertainty through very complex and large models.

REFERENCES

[Adams, 2003] Adams, D., Interview by author, November, 2003.

[Ahmed, 2003] Ahmed, A., Interview by author, September, 2003.

[Apostolakis & Michal, 2000] Apostolakis, G. and Michal, R., "Apostolakis: On PRA," *Nuclear News*, Vol. 43, No. 3, 2000, pg. 27-31.

[Arunajadai et al, 2002] Arunajadai, S., Stone, R., and Tumer, I., "A Framework for Creating a Function-Based Design Tool for Failure Mode Identification," *Proceedings of DETC'02 ASME 2002 Design Engineering Technical Conference and Computers and Information in Engineering Conference,* DETC2002/DTM-34018, Montreal, Canada, Oct. 2002.

[Babcock, 1986] Babcock, P.S., *An Introduction to Reliability Modeling of Fault-Tolerant Systems*. The Charles Stark Draper Laboratory, Inc., Technical Report, Cambridge, MA, September 1986.

[Chhikara et al, 2003] Chhikara, R., Heydorn, R., and Pitblado, J., "Probabilistic Risk Assessment Using Dynamic Event Sequence Diagrams", The University of Houston [Online], Available at: http://www.isso.uh.edu/publications/A9900/mini-chhikara-2.htm, September 2003.

[Ciardo et al, 1990] Ciardo, G., Marie, R., Sericola, K., and Trivedi, K., "Performability Analysis Using Semi-Markov Reward Processes," *IEEE Transactions on Computers*, Vol. 39, No. 10, 1990, pp. 1251-1264.

[Ciciani & Vincenzo, 1987] Ciciani, B., and Vincenzo, G., "Performability Evaluation of Fault-Tolerant Satellite Systems," *IEEE Transactions on Communications*, Vol. COM-35, No. 4, 1987, pp. 403-409.

[Cojazzi, 1996] Cojazzi, G., "The DYLAM Approach for the Dynamic Reliability Analysis of Systems," *Reliability Engineering and System Safety*, Vol. 52, 1996, pp. 279-296.

[DeLaurentis & Mavris, 2000] DeLaurentis, D. and Mavris, D., "Uncertainty Modeling and Management in Multidisciplinary Analysis and Synthesis," *Proceedings of the 38th Aerospace Sciences Meeting & Exhibit,* AIAA-2000-0422, Reno, NV, Jan. 2000.

[Devooght & Smidts, 1996] Devooght, J. and Smidts, C., "Probabilistic Dynamics as a Tool for Dynamic PSA," *Reliability Engineering and System Safety*, Vol. 52, 1996, pp. 185-196.

[Dubovitsky, 2004] Dubovitsky, S., Lay, O., et. al., *Terrestrial Planet Finder Interferometer Strawman Configurations*. Darwin/TPF Interferometer Design Team Meeting, Saas Fee, Switzerland, February 2004.

[Dubovitsky, 2004] Dubovitsky, S., and Lay, O., "Architecture Selection and Optimization for Planet-Finding Interferometers," *Proceedings of the 2004 SPIE Astronomical Telescopes and Instrumentation Conference,* Glasgow, Scotland, June 2004.

[Ebbeler et al, 2003] Ebbeler, D., Aaron, K., Fox, G., and Walker, W., "Space Interferometer Reliability-Based Design Evaluation," *Case Studies in Reliability and Maintenance*, Blischke, W. and Murthy, D. (eds)., John Wiley & Sons, New York, NY, 2003.

[ESA, 2004] ESA's Strawman Configurations. Darwin/TPF Interferometer Design Team Meeting, Saas Fee, Switzerland, February 2004.

[Fisher & Miller, 2003] Fisher, D., and Miller, D., Interview by author, December, 2003.

[Gunter, 2005] Gunter, S., Interview by author, February, 2005.

[Hamlin, 2005] Hamlin, L., Interview by author, April, 2005.

[Hassan & Crossley, 2003] Hassan, R. and Crossley, W., "Comparison of Sampling Techniques for Reliability-Based Optimization of Communication Satellites Using Genetic Algorithms," AIAA-2003-1332, 2003.

[Henry, 2003] Henry, C., "Interferometry 101", JPL Internal Presentation, May 2003.

[Henry, 2005] Henry, C., Interview by author, March, 2005.

[Hoyland & Rausand, 1994] Hoyland, A. and Rausand, M., *System Reliability Theory: Models and Statistical Methods*, John Wiley & Sons, New York, NY, 1994.

[Jilla, 2002] Jilla, C., *A Multiobjective, Multidisciplinary Design Optimization Methodology for the Conceptual Design of Distributed Satellite Systems*. Massachusetts Institute of Technology Space Systems Laboratory, Doctoral Thesis, Cambridge, MA, May 2002.

[JPL, 2003] Jet Propulsion Laboratory Professional Development, "The JPL Project Risk Management Workshop," JPL Internal Document, JPL D-21069 Rev. G., Pasadena, CA, Dec. 2003.

[JPL, Galileo, 2005] Jet Propulsion Laboratory, "Galileo Mission to Jupiter", [Online], Available at: http://jpl/news/fact_sheet/galileo.pdf, January 2005.

[JPL, Genesis, 2005] Jet Propulsion Laboratory, "Genesis Mission Status Report", [Online], Available at: http://genesismission.jpl.nasa.gov/mission/status_report.html, January 2005.

[JPL, TPF, 2005] Jet Propulsion Laboratory, "Terrestrial Planet Finder?", [Online], Available at: http://planetquest.jpl.nasa.gov/TPF/tpf_index.html, August 2005.

[Lawson & Dooley, 2005] Lawson, P., and Dooley, J., "Technology Plan for the Terrestrial Planet Finder Interferometer", Jet Propulsion Laboratory Publication 05-5, Pasadena, CA, June 2005.

[Lay et al, 2005] Lay, O., Gunter, S., Hamlin, H., Henry, C., Li, Y., Martin, S., Purcell, G., Ware, B., Wertz, J., and Noecker, C., "Architecture Trade Study for the Terrestrial Planet Finder Interferometer", *Proceedings of the 2005 Optics and Photonics SPIE Conference*, San Diego, CA, Aug. 2005.

[Lay, 2001] Lay, O., Interview by author, June, 2001.

[Lay, 2005] Lay, O., Interview by author, February, 2005.

[Lay, August 2005] Lay, O., Interview by author, August, 2005.

[Lindsey, 1998] Lindsey, N., "L2 Natural Environment Summary", [Online], Available at:http://maxim.gsfc.nasa.gov/documents/Mission_Concept_Work/ISAL_January_2002_SST/SST_ISAL-1/Super_Star_Tracker/L2-natural-environment.pdf, August 2005.

[Martin, 2005] Martin, S., Interview by author, February, 2005.

[Meshkat & Scherbenski, 2005] Meshkat, L. and Scherbenski, J., "A Case Study for Risk Assessment & Modeling in Conceptual Concurrent Design," Jet Propulsion Laboratory Internal Document, Pasadena, CA, 2005.

[Meshkat et al, 2003] Meshkat, L., Xing, L., Donohue, S., and Ou, Y., "An Overview of the Phase-Modular Fault Tree Approach to Phased Mission System Analysis," *Proceedings of theInternational Conference of Space Mission Challenges for Information Technology,* SMC-IT 2003, 2003.

[Meyer, 1980] Meyer, J.F., "On Evaluating the Performability of Degradable Computing Systems," *IEEE Transactions on Computers*, Vol. C-29, 1980, pp. 720-731.

[Miller, 2001] Miller, D., Interview by author, July, 2001.

[Miller, 2004] Miller, D., Sedwick, R., Wertz, J., Kwon, D., and Lobosco, D., *TPF Interferometer Trades Model Development Final Report*, MIT Space Systems Laboratory, Technical Report submitted to the Jet Propulsion Laboratory, Cambridge, MA, August 2004.

[Paulos, 2005] Paulos, T., "Introduction to Probabilistic Risk Assessment Using SAPHIRE," Jet Propulsion Laboratory Professional Development Course, Pasadena, CA, April 2005.

[Rahman, 2003] Rahman, Z., Interview by author, September, 2003.

[Relex, 2005] Relex Software Corporation, "Fault Tree Analysis Software, Decision & Fault Tree Analysis", [Online], Available at: http://www.relexsoftware.com/resources/art/art_fta3.asp, June 2005.

[Roberts, 2001] Roberts, B., "The Benefits of Integrated, Quantitative Risk Management," *Proceedings of the 12th Annual International Symposium of the International Council on Systems Engineering*, Melbourne, Victoria, Australia, July 2001.

[Rumsey, 2003] Rumsey, D., *Statistics for Dummies*, Hungry Minds, New York, NY, 2003.

[Siu, 1994] Siu, N., "Risk Assessment for Dynamic Systems: An Overview," *Reliability Engineering and System Safety*, Vol. 43, 1994, pp. 43-73.

[Smith et al, 1988] Smith, R.M., Trivedi, K.S., and Ramesh, A.V., "Performability Analysis: Measures, an Algorithm, and a Case Study," *IEEE Transactions on Computers*, Vol. 37, No. 4, 1988, pp. 406-417.

[Smith et al, 2002] Smith, C., Knudsen, J., Kvarfordt, K., and Wood, T., "SAPHIRE Basics: An Introduction to Probabilistic Risk Assessment via the SAPHIRE Software," Idaho National Engineering and Environmental Laboratory, Fall 2002.

[Stamatelatos, 2002] Stamatelatos, M., "Probabilistic Risk Assessment (PRA) at NASA: Past, Present, and Future," Presented at the Jet Propulsion Laboratory, Pasadena, CA, Feb. 2002.

[Tien, 2003] Tien, J., Interview by author, September, 2003.

[Tumer & Stone, 2001] Tumer, I. and Stone, R., "Mapping Function to Failure Mode During Component Development," *Proceedings of the DETC 2001,* DETC2001-DFM21173.

[Walton & Hastings, 2001] Walton, M. and Hastings, D., "Quantifying Embedded Uncertainty of Space Systems Architectures in Conceptual Design," *Proceedings of the AIAA Space 2001 Conference and Exhibition,* AIAA-2001-4573, Albuquerque, NM, Aug. 2001.

[Wang et al, 2004] Wang, W., Loman, J., and Vassiliou, P., "Reliability Importance of Components in a Complex System," *Proceedings of the 2004 IEEE Reliability and Maintainability Symposium,* Los Angeles, CA, Jan. 2004.

[Wertz, 2002] Wertz, J., *Reliability and Productivity Modeling for the Optimization of Separated Spacecraft Interferometers.* Massachusetts Institute of Technology Space Systems Laboratory, Masters of Science Thesis, Cambridge, MA, June 2002.

[Wertz, 2005] Wertz, J. and Miller, D., *A New Approach to Modeling the Expected Productivity of Path-Dependent Systems*, MIT Space Systems Laboratory, Internal Report, Cambridge, MA, January 2005.

[Wilhite et al, 2003] Wilhite, A., Odom, P., Lovell, N., and Lord, R., "Estimating the Risk of Technology Development," *Presented at the American Society of Engineering Management*, September 2003.

[Wolfram, 2005] Wolfram Research, "Union", [Online], Available at: http://mathworld.wolfram.com/Union.html, June 2005.

Appendix A

Full TPF-I Risk List

The process of identifying risk items for the TPF-I mission was discussed in Chapter 6. As mentioned in Chapter 6, once completed, the risk list was organized in to a tree-like structure. It is important to note that the tree-structure and categories are for organizational purposes only. They are used to help organize the list of risk items and to clarify the risk list when showing design team members and managers. The categories and tree-structure do not affect the results of the risk model, in terms of the expected number of observations completed.

The full TPF-I risk is shown in Table A-1. Note that in Table A-1, *Oe* is the observational efficiency, *Pcoll* is the probability of collision, *Pevap* is the probability of evaporation, *MaxBase* and *MinBase* are the maximum and minimum baseline lengths allowed respectively, *IntTime* is the integration time, *Pthlk_es* is the probability of a thermal leak due to excess sources on the cold side, *Life* is the lifetime of the mission, *Pnotime* is the probability of not having enough time between disturbances to complete an observation, *Pvibe* is the probability of vibrations due to self-induced disturbances, spc stands for spacecraft, comb stands for combiner, and coll stands for collector.

The tree-structure organization for the risk list is shown in Figures A-1 through A-14. In Figures A-1 through A-14, the boxes are color-coded according to probability. Additionally, a solid border means the failure mode is critical, no border means a degraded state failure mode, and a dashed border implies the failure mode could be either degraded state or critical. A detailed discussion of the individual risks to the TPF-I mission, organized into the categories shown in Figures A-1 through A-14, is given in Chapter 6.

Table A- 1: Full TPF-I risk list

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
1	a	1			ACS Failure	Spc Lost	N/A	See below	See below	See below	See below	Spacecraft		
1	a	1	a		Star-tracker failure	ACS failure	Either	Throughout Life	1	Very Low	0.1%	Spacecraft		Proven component
1	a	1	b		Gyro failure	ACS failure	Either	Throughout Life	1	Very Low	0.1%	Spacecraft		Proven component
1	a	1	c		Sensor failure	ACS failure	Either	Throughout Life	1	Very Low	0.1%	Spacecraft		Proven component
1	a	2			Computer failure	Spc Lost	Either	Throughout Life	1	Very Low	0.1%	Spacecraft		Test at high radiation /cryogenic environs.
1	a	3			Meteoroid strike	Spc Lost	Either	Throughout Life	Unique	Unique	0.00066%	Spacecraft		Prob. Needs to be multiplied by exposed area

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
1	a	4	a		Sunshield deploy failure	Spc lost	Either	Single Event	3	Very Low	0.1%	Spacecraft	8 deploy-ments	5 sunshades per spc. Deployed out of 4 booms, all 5 shades together. Then each section is spread using a spreader bar.
1	a	4	b		Solar array deploy failure	Spc Lost	Either	Single Event	3	Very Low	0.1%	Spacecraft	4 deploy-ments per spc	
1	a	4	c		HGA deploy failure	Oe = Oe/3	Degraded	Single Event	3	Very Low	0.1%	Combiner		Assume you get data down at a lower rate, but can still get the data down using collector antennas

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
1	a	4	d		Cryo Radiator deploy failure	1 failure per spc.: Int_time = Int_time x2 or loss of spc., 2 or more failures per spc. = Spc lost	Either	Single Event	3	Very Low	0.1%	Spacecraft	6 deploy-ments	Degraded state results in increased noise photons, leading to IntTime = IntTime*2.
1	a	5			Hit by other mission in L2	Spc lost	Either	Throughout life	Unique	Unique	0.00066%	Spacecraft		No probability numbers available. Assumption is that the probability would be on the same order as being hit by a meteoroid.

ID No.						Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
1	a	6				DTE Comm. failure	Oe = Oe/2	Degraded	Throughout life	1	Very Low	0.1%	Combiner		There is redundancy in that all 4 collectors will have some reduced DTE capability.
1	b	1				Loss of control of secondary mirror	Spc Lost	Either	Throughout Life	6	Low	0.5%	Collectors		Control requirement is very strict (no exact heritage).
1	b	2				Metrology failure	Spc payload lost	See below	N/A	See below	See below	See below	Spacecraft	N/A	

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
1	b	2	a		Intensity Gradient Detector Failure	Spc payload lost	Either	Single Event	2	Low	0.5%	Spacecraft	9 mecha-nisms total	IGDs: 1 on collector 1, 4 on collector 2, 3 on collector 3, 1 on collector 4, and 0 on combiner. Note that is assumed that since there are no moving parts on an IGD, the system will not fail throughout the lifetime.
1	b	2	b		Fast steering tip/tilt mirror failure	Spc payload lost	Either	Throughout Life	1	Very Low	0.1%	Spacecraft	13 comp-onents total	Mirrors: 1 on collector 1, 3 on collector 2, 4 on collector 3, 1 on collector 4, 4 on combiner

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
1	b	2	c		Metrology alignment mirrors	Starlight beam lost	Either	Throughout Life	1	Very Low	0.1%	Collectors	2 mirrors per beam or col.	Each metrology beam has an alignment mirror. 2 alignments per starlight beam. Won't be active during observation. A failure results in the loss of that starlight beam, which is equivalent to the loss of that collector.
1	b	2	d		Metrology laser failure	Payload Lost	Complete	Throughout Life	1	Very Low	0.1%	Combiner	2 lasers	
1	b	3			Optical path compo-nent failure	N/A	N/A	N/A	See below	See below	See below	See below		
1	b	3	a		Field of regard mirror failure	Coll. payload lost	Either	Throughout Life	1	Very Low	0.1%	Collectors		

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
1	b	3	b		Pointing alignment mirror	Coll. payload lost	Either	Throughout Life	1	Very Low	0.1%	Collectors		Allow pointing light to align with Starlight
1	b	3	c		Alignment mirror	Coll. payload lost	Either	Single Event	1	Very Low	0.1%	Collectors		Moves once prior to operations and then locks in place
1	b	3	d		Transfer mirror	Coll. payload lost	Either	Throughout Life	1	Very Low	0.1%	Collectors		
1	b	3	e		Mirror w/ sensors	Inner Coll. payload lost	Complete	Throughout Life	1	Very Low	0.1%	Inner Collectors		
1	b	3	f		Fine Guidance sensor failure	Coll. payload lost	Either	Single Event	1	Very Low	0.1%	Collectors		Assume the FGS is a quad cell (no moving parts). Could also be a camera.
1	b	3	g		Wavefront sensor failure	Coll. payload lost	Either	Throughout Life	1	Very Low	0.1%	Collectors		Assume the WFS is a camera with moving parts that could fail throughout life.

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
1	b	3	h		Co-alignment sensor failure	Coll. payload lost	Either	Single Event	1	Very Low	0.1%	Collectors		Assume the CAS is a quad-cell with no moving parts.
1	b	3	i		Combiner alignment mirror failure	Payload lost	Complete	Throughout Life	1	Very Low	0.1%	System	4 mirrors	3 mirrors inside combiner, 1 at input to combiner
1	b	4	a		Secondary mirror deploy failure	Coll. payload lost	Either	Single Event	4	Low	0.5%	Collectors	4 coll.	
1	b	4	b		Straylight baffle deploy	Max Base = Max Base/2 or Loss of spc.	Degraded	Single Event	4	Low	0.5%	Spacecraft	1 on spc. 1 and 4, 3 on spc. 2 and 3, 2 on comb.	Impact depends on which is better - removing the spacecraft from array or decreasing maximum baseline.
1	b	5			Optical lock-down mech. for launch doesn't open	Spc lost	Either	Single Event	3	Very Low	0.1%	Spacecraft		Similar to a deployment.

ID No.	Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
1 b 6	Contam-ination due to control system error	Spc payload lost	Either	Throughout Life	7	Med	1.0%	Spacecraft		Total probability is normal for category 7 - medium. However, the impact varies based on which spacecraft was contam-inated. The probability for each spacecraft having contam-ination from each thruster pointed in its direction is assumed to be equal - leading to P/6 for the outer collectors and P/3 for the inner collectors.

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
1	b	7			Fringe Tracking camera failure	Payload Lost	Complete	Throughout Life	1	Very Low	0.1%	System	2 cams	Not redundant
1	b	8			ODL failure	Payload Lost	N/A	See below	See below	See below	See below	System	Will have 4 ODLs, need 3	
1	b	8	a		ODL sensor failure	ODL failure	Either	Throughout Life	2	Low	0.5%	System		
1	b	8	b		ODL course stage actuator	ODL failure	Either	Throughout Life	2	Low	0.5%	System		
1	b	8	c		ODL voice coil	ODL failure	Either	Throughout Life	2	Low	0.5%	System	2 voice coils	
1	b	8	d		ODL piezo	ODL failure	Either	Throughout Life	2	Low	0.5%	System	2 piezos	
1	b	8	e		ODL interface hardware failure	ODL failure	Either	Throughout Life	2	Low	0.5%	System		
1	b	8	f		ODL software failure	ODL failure	Either	Throughout Life	2	Low	0.5%	System		
1	b	9			Nulling camera	Payload Lost	Complete	Throughout Life	1	Very Low	0.1%	System		Science camera.

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
1	b	10			Detectors less sensitive than expected	Oe = Oe/2	Degraded	Single Event	1	Very Low	0.1%	System	3 types	Source of failure could be radiation damage. Note that mission critical level failures are accounted for with each individual type of detector.
1	b	11			Internal test mirror stuck	Mission Lost	Complete	Single Event	1	Very Low	0.1%	Combiner		Mirror to calibrate or run internal tests gets stuck over input to combiner blocking all external light.
1	b	12			Variable phases mech-anism fails	Stuck in deg or non-deg modes	Degraded	Single Event	1	Very Low	0.1%	Combiner		May be possible to add redundancy.
1	b	13			Cryo-cooler failure	Comb. failure	Complete	Throughout Life	2	Low	0.5%	Combiner		1 cryocooler on combiner only

ID No.	Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
1 b 14	Hi-low res switch failure	Stuck in high or low res mode (50%) or Mission failure (50%)	Either	Throughout Life	1	Very Low	0.1%	Combiner		Can fail so stuck in either position, or so blocks both positions.
1 b 15	Quality of primary bad	Spc payload lost	Degraded	Single Event	1	Very Low	0.1%	Collector payload		Note that no signal could be received from a bad inner collector, but signals could still be passed through.
1 b 16	Quality of secondary bad	Spc payload lost	Degraded	Single Event	1	Very Low	0.1%	Collector payload		Note that no signal could be received from a bad inner collector, but signals could still be passed through.

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
1	c	1			AFF antenna failure	Pcoll = Pc*5 Pevap = Pevap*5 Oe = Oe/1.5 Min Base = Min Base*2	Either	Throughout Life	1	Very Low	0.1%	Spacecraft	n_ant	If up to two antennas fail. More than two failed antennas leads to complete AFF system failure for that spacecraft. Note, includes both antennas and modules. Usual n_ant = 12

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
1	c	2			AFF transmitter failure	Pcoll = Pc*5 Pevap = Pevap*5 Oe = Oe/1.5 Min Base = Min Base*2	Either	Throughout Life	1	Very Low	0.1%	Spacecraft	n_trans	If up to two transmitters fail. More than two failed transmitters leads to complete AFF system failure. Note, includes both transmitters and modules. Usual n_trans = 4
1	c	3			AFF baseband processor failure	Spc Lost	Either	Throughout Life	1	Very Low	0.1%	Spacecraft		Complete AFF System Failure.
1	c	4			AFF frequency subsystem failure	Spc Lost	Either	Throughout Life	1	Very Low	0.1%	Spacecraft		Complete AFF System Failure.
1	c	5			AFF power subsystem failure	Spc Lost	Either	Throughout Life	1	Very Low	0.1%	Spacecraft		Complete AFF System Failure.

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
1	c	6			AFF actuator failure	Pcoll = Pc*5 Pevap = Pevap*5 Oe = Oe/1.5 Min Base = Min Base*2 or Mission Lost	Either	Throughout Life	1	Very Low	0.1%	Spacecraft	n_act	Impact defined by redundancy.
2	a	1			ACS Estimation (software) failure	ACS failure	Either	Throughout Life	1	Very Low	0.1%	System		Assume any software error will be systematic, and therefore will affect the entire system.

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
2					Thermal leak to cold side	1 source: IntTime = IntTime* 2, 2 or more sources = Mission critical	N/A	See below	See below	See below	See below	System		Probability value based on number of sources of leaks. 1 source = degraded failure. 2 or more sources = mission critical failure. Few degree temperature rise -> 2x noise photons -> 2x integration time.
2	a	2			Thermal leak from lack of shielding	See 1f above	Degraded	Single Event	6	Low	0.5%	System		Considered only similar heritage since requirement on thermal leaks are so tight.

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
2	a	2	b		Thermal leak from power/ electrical lines	See 1f above	Degraded	Single Event	6	Low	0.5%	System		Considered only similar heritage since requirement on thermal leaks are so tight.
2	a	2	c		Thermal leak from excess sources on cold side	See 1f above	Degraded	Single Event	8	Med	1.0%	System		Considered only similar heritage since requirement on thermal leaks are so tight. Increased probability category due to design team concern (Hamlin)
2	a	2	c	1	Placement of subsystem s leads to thermal issues	Pthlk_es = Pthlk_es *5	Degraded	Single Event	5	Very Low	0.1%	System		Other subsystems include AFF system, ISC system, Thrusters, ODL actuators, etc.

ID No.				Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
2	a	3		Higher outgasing than expected	Life = Life/2	Degraded	Single Event	5	Very Low	0.1%	System		
2	a	4		Operator error	Mission Lost	Complete	Throughout life	5	Very Low	0.1%	System		Includes sending the wrong command to the wrong spacecraft.
2	b	1		Bad data - "identify" non-planets	N/A	N/A	See below	See below	See below	See below	System		Oe adjusted to assume only get science value out of 1/2 of observations Oe = science/(science + overhead) = s/(s+ o). Oe_adj = s/2(o+s) = Oe/2.
2	b	1	a	Exozodi has "lumps" in it	Oe = Oe/2	Degraded	Single Event	7	Med	1.0%	System		

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
2	b	1	b		Contami-nation of spectra by unseen planets or bodies	Oe = Oe/2	Degraded	Single Event	7	Med	1.0%	System		
2	b	1	c		Planetary extraction algorithms don't work.	Oe = Oe/2	Degraded	Single Event	7	Med	1.0%	System		
2	b	2			Not enough time between distur-bances for obser-vations	Mission Lost	Complete	Single Event	7	Med	1.0%	System		

ID No.				Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
2	b	3		Contami-nation from self out-gasing	Mission lost	Complete	Single Event	7	Mediu m	1.0%	System		Note that this is from nominal operations - assumes models of thrusters are wrong, etc. Assume this would be a systematic error and would therefore effect all 4 collectors, leading to a total loss of mission.
2	b	4		Thermal induced optical mis-alignments	Life = Life/1.1, Oe = Oe/2	Degraded	Single Event	5	Very Low	0.1%	System		Oe increased to account for situations where there no longer exists enough control band to remove certain disturbances.

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
2	b	5			Excess or un-expected sources of straylight	Oe = Oe/2 (50%) or Mission Critical (50%)	Either	Single Event	7	Med	1.0%	System		
2	b	6			Beam Walk	Mission Lost	Complete	Single Event	7	Med	1.0%	System		
2	c	1			AFF estimation (software) failure	Mission Lost	Complete	Throughout Life	2	Low	0.5%	System		Assume any software error is systematic and would therefore affect all spacecraft, resulting in loss of mission. Note this is an untraceable and unfixable software error.
2	c	2			Inter-spacecraft comm failure	Mission Lost	Complete	Throughout Life	1	Very Low	0.1%	System		

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
2	c	3			Slow inter-spacecraft comm link	Oe = Oe/1.5, Pnotime = 2x Pnotime	Degraded	Single Event	6	Low	0.5%	System		Note this is assuming ISC system is developed to meet requirement.
2	c	4			Collision	Mission Lost	Complete	Throughout Life	7	Med	1.0%	System		Assumes algorithms developed correctly. Largest public perceived risk. Note that this needs to be a probability by end of life since it is affected by other failure modes. It is changed to a failure rate after effects have been considered.

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
2	c	5			Evap-oration	Mission Lost	Complete	Throughout Life	7	Med	1.0%	System		Note that this needs to a probability by end of life since it is affected by other failure modes. It is changed to a failure rate after effects have been considered.
2	c	6			Formation acquisition failure	Mission Lost	Complete	Single Event	7	Med	1.0%	System		
2	c	7			Handoff between sensors doesn't work	Mission Lost	Complete	Single Event	7	Med	1.0%	System		No handoff means the fine sensors don't get a chance - no way to track a fringe.

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
2	d	1			Vibration during ops from self-induced distur-bances	1 source: Oe = Oe/2, Pnotime = 2x Pnotime 2 or more sources: Mission critical	N/A	Single Event	See below	See below	See below	System		
2	d	1	a		Dist from reaction wheels	See above	Degraded	Single Event	5	Very Low	0.1%	System		
2	d	1	b		Dist from cryo-pump	See above	Degraded	Single Event	5	Very Low	0.1%	System		
2	d	1	c		Dist from thermal snap	See above	Degraded	Single Event	5	Very Low	0.1%	System		
2	d	1	d		Dist from moving optics	See above	Degraded	Single Event	5	Very Low	0.1%	System		

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
2	d	1	e		Dist from thrusters	See above	Degraded	Single Event	8	Med	1.0%	System		Note that this may require a sensitivity study. Difference in opinion between design team members as to the likelihood of the event occurring.
2	d	1	f		Placement of other sub-systems causes structural control issues	See above	Degraded	Single Event	5	Very Low	0.1%	System		Possible sources include AFF system, ISC system, propulsion system, etc.

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
2	d	2			Excess or un-expected control noise sources	Oe = Oe/2, Pnotime = 2x Pnotime (50%) or Mission Critical (50%)	Either	Single Event	8	Med	1.0%	System		Could include ultra-low amplititude, high frequency vibrations. Modeling does not capture this effect yet. Concern from Henry.
2	d	3			Plant dynamics changing due to fuel slosh	Oe= Oe/1.5	Degraded	Single Event	5	Very Low	0.1%	System		Changes from fuel usage, fuel slosh, etc. Has to be significant enough to not be corrected for.
2	d	4			Plume impinge-ment restricts control directions	Oe = Oe/2	Degraded	Single Event	7	Med	1.0%	System		

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
2	d	5			Unsensed mode	Mission lost	Complete	Single Event	7	Med	1.0%	System		Assume the mode can not be corrected for.
2	e	1			Structural failure during launch	Mission Lost	Complete	Single Event	5	Very Low	0.1%	System		May be some function of the center of gravity.
2	e	2			Failures or mis-alignments from accel loads at launch	Mission Lost	Complete	Single Event	5	Very Low	0.1%	System		Mis-alignment needs to be out of control range.
2	e	3			Miss L2 Injection	Mission Lost	Complete	Single Event	5	Very Low	0.1%	System		
2	e	4			Constell-ation deploy failure	Mission Lost	Complete	Single Event	5	Very Low	0.1%	System	5 deploy-ments	Each spacecraft deploys separately. Includes tip-off during spacecraft deployment.
2	e	5			Launch failure	Mission Lost	Complete	Single Event	Unique	Unique	6.5%	System		P = 0.065 based on Delta LV (174 successes out of 186 attempts).

ID No.			Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
2	e	6	Cruise stage failure	Mission Lost	Complete	Single Event	1	Very Low	0.1%	System		
2	e	7	Unknown unknowns from system of systems and inability to test on ground	Mission Lost	Complete	Single Event	7	Med	1.0%	System		
2	e	8	Wrong require-ments	Mission Lost	Complete	Single Event	7	Med	1.0%	System		Assuming require-ments are wrong to level of mission failure. Too many degraded states to account for all otherwise.
2	e	9	Mis-handling during ATLO	Mission Lost	Complete	Single Event	5	Very Low	0.1%	System		

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
3	a				Single mode spatial filtering not developed to required levels.	Oe = Oe/3	Degraded	Single Event	12	High	5.0%	System		
3	b				Adaptive nulling not developed to required levels.	Oe = Oe/3	Degraded	Single Event	12	High	5.0%	System		
3	c				AFF does not meet require-ments	Pcoll = Pcoll*5 Pevap = Pevap*5 Oe = Oe/2 Min Base = Min Base*2	Degraded	Single Event	12	High	5.0%	System		-
3	d				ISC not developed to meet latency require-ments	Oe = Oe/1.5, Pnotime = 2x Pnotime	Degraded	Single Event	10	Med	1.0%	System		Relatively well understood subsystem. Less strict require-ments than other subsystems.

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
3	e				Formation flight algorithms not developed	Pcoll = Pcoll*5 Pevap = Pevap*5 Min Base = Min Base*2	Degraded	Single Event	12	High	5.0%	System		Note that this may be mission critical - there may not exist a degraded mode that is capable enough to lead to any productivity.
3	f				Formation autonomy technology not developed	Pcoll = Pcoll*5 Pevap = Pevap*5 Oe = Oe/2 Min Base = Min Base*2	Degraded	Single Event	12	High	5.0%	System		Note that this may be mission critical - there may not exist a degraded mode that is capable enough to lead to any productivity.
3	g				Instrument Control technology (PDT) does not meet require-ments	Oe = Oe/2, Pnotime = 2x Pnotime	Degraded	Single Event	11	Very High	10.0%	System		Very strict require-ments to meet.

ID No.					Risk Event	Impact	Degraded or Complete Failure	Single Event or Throughout Life	Prob. Cat. ID	Prob. Bin	Prob. Value	System, Collectors, Spacecraft	# of Spc. or Sys.	Comments
3	h				Testing/ modeling not conclusive about cryogenic structures	Pvibe = Pvibe*5	Degraded	Single Event	7	Med	1.0%	System		
3	i				No material found which damps vibrations in cryogenic structures	Pvibe = Pvibe*5	Degraded	Single Event	10	Med	1.0%	System		
3	j				Implication of instability at L2 not well understood prior to launch	Oe = Oe/2, Pnotime = 2* Pnotime Pcoll = Pcoll*2 and Pevap = Pevap*2	Degraded	Single Event	6	Low	0.5%	System		

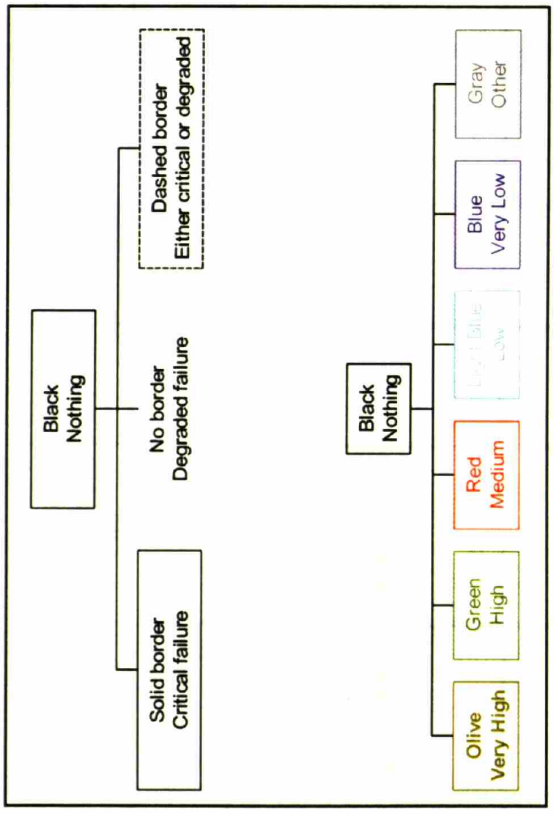


Figure A- 1: Key for Figures A2-A14

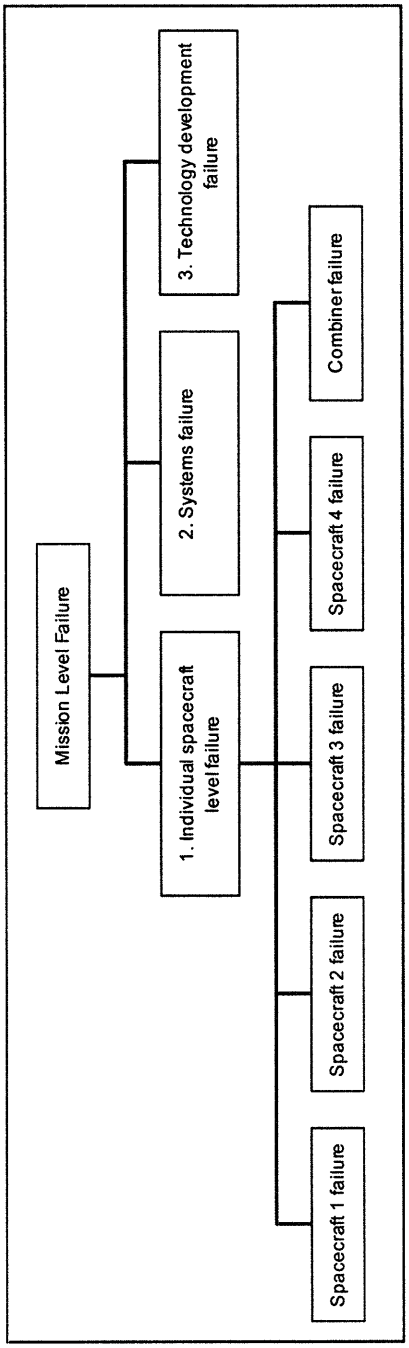


Figure A- 2: Mission level failures

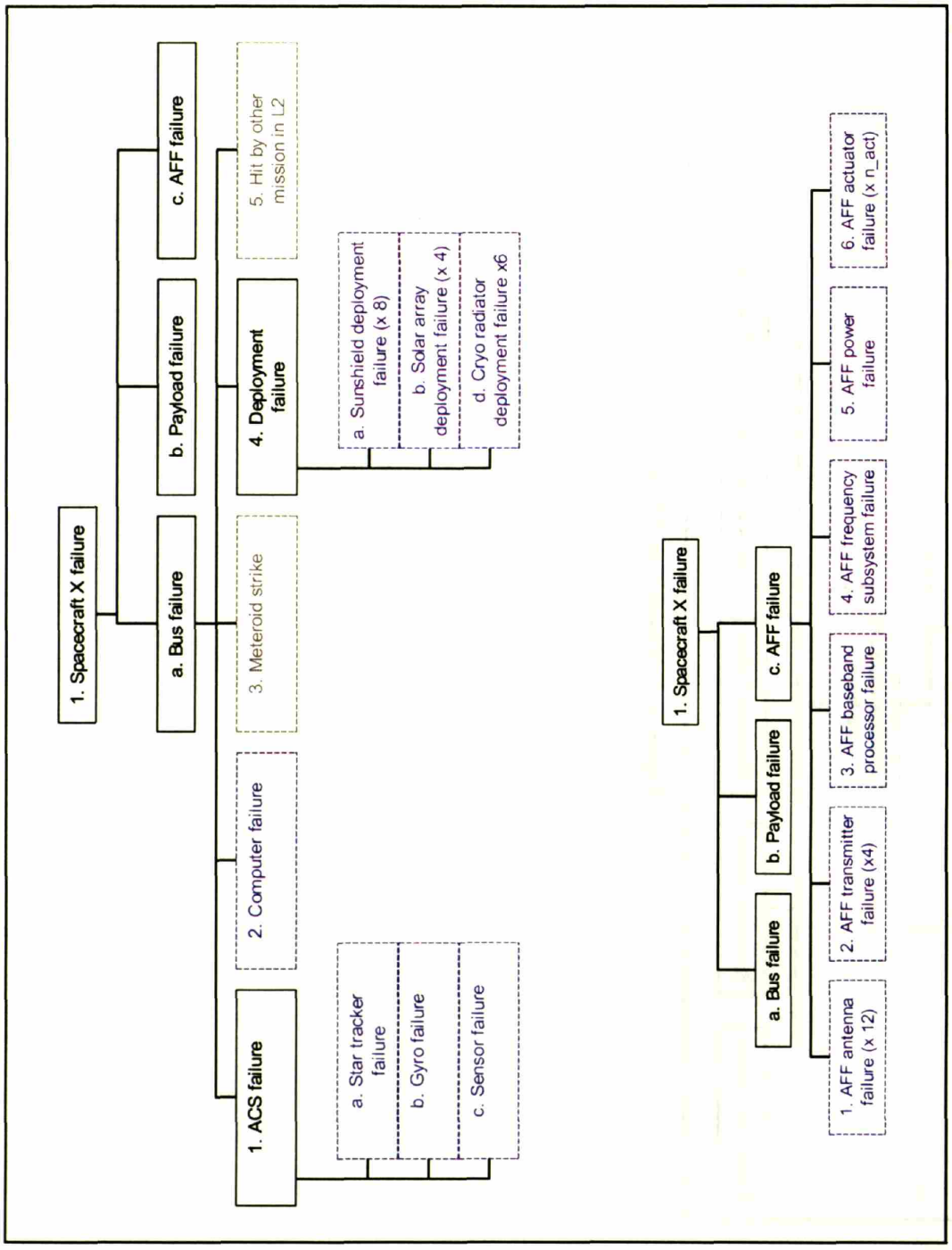


Figure A- 3: : Spacecraft level failures common to all spacecraft

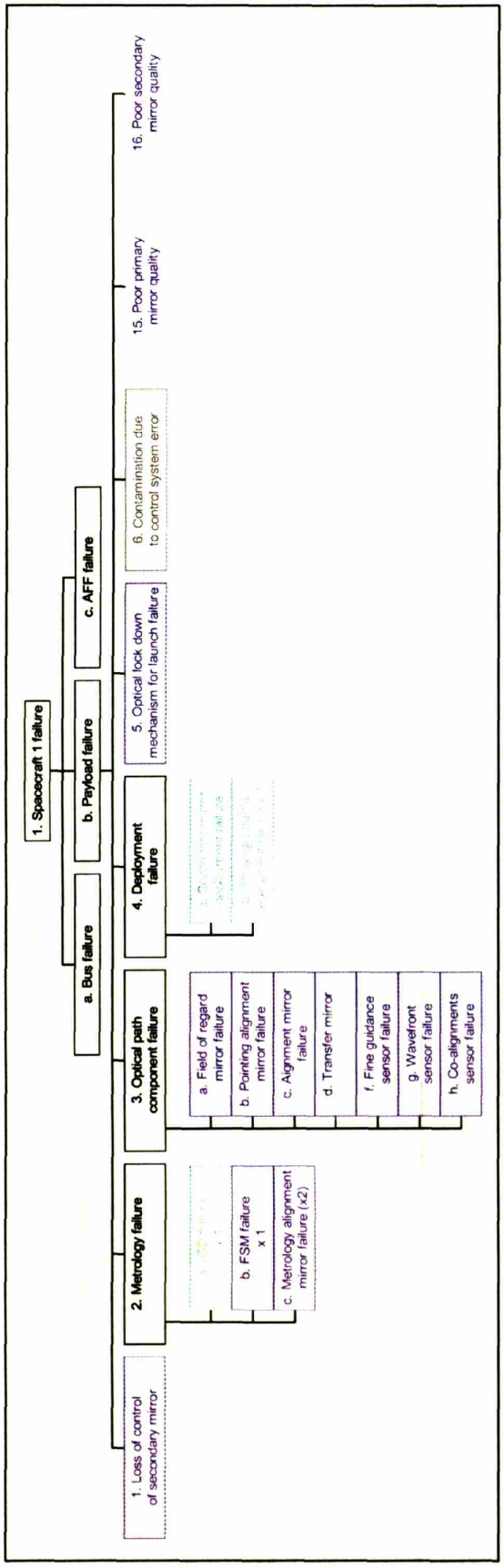


Figure A- 4: Failures specific to Spacecraft 1

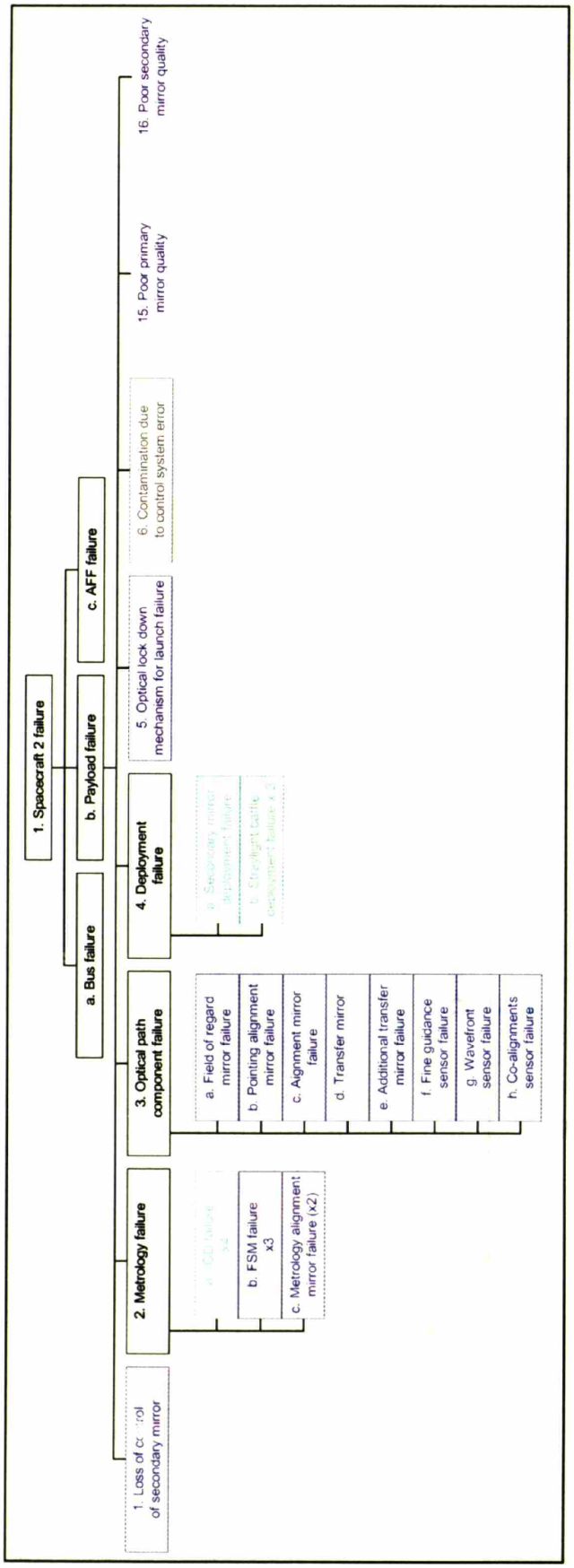


Figure A- 5: Failures specific to Spacecraft 2

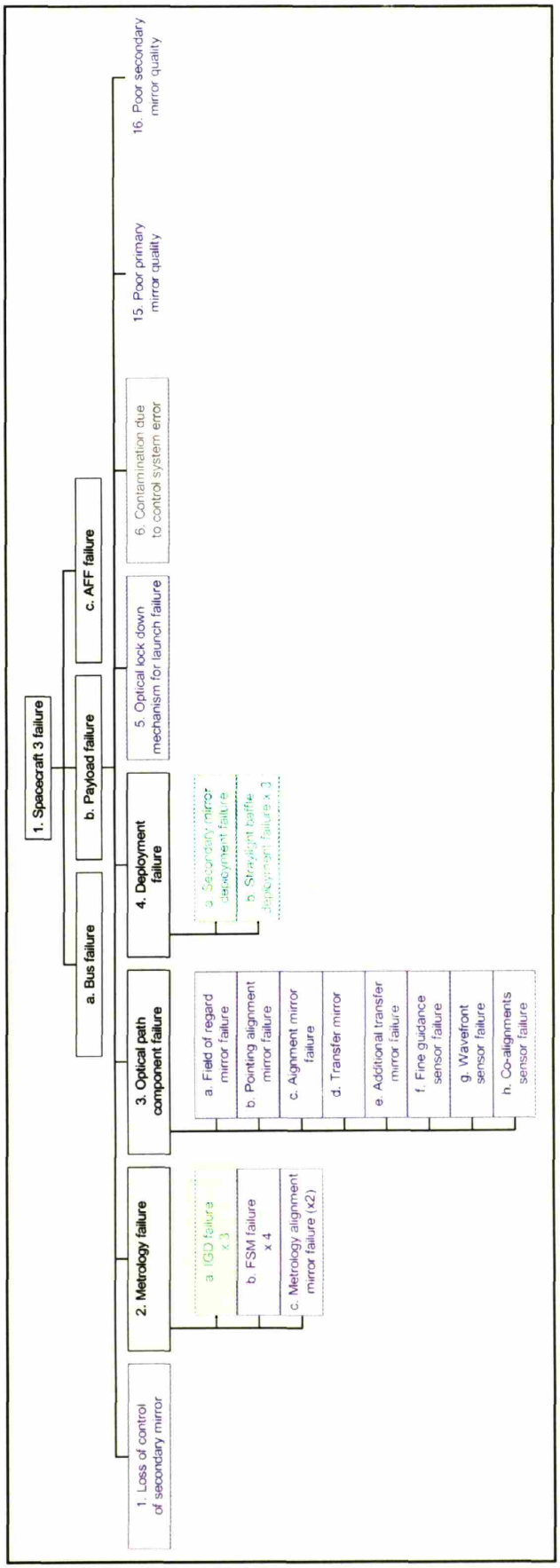


Figure A- 6: Failures specific to Spacecraft 3

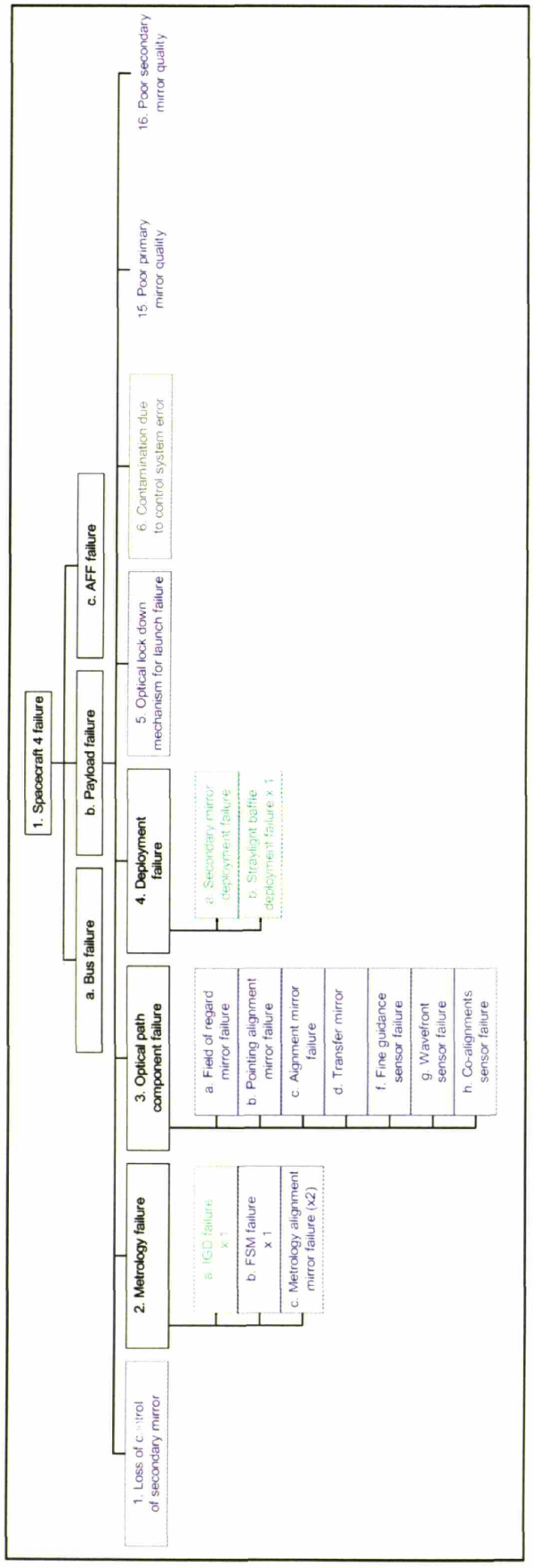


Figure A- 7: Failures specific to Spacecraft 4

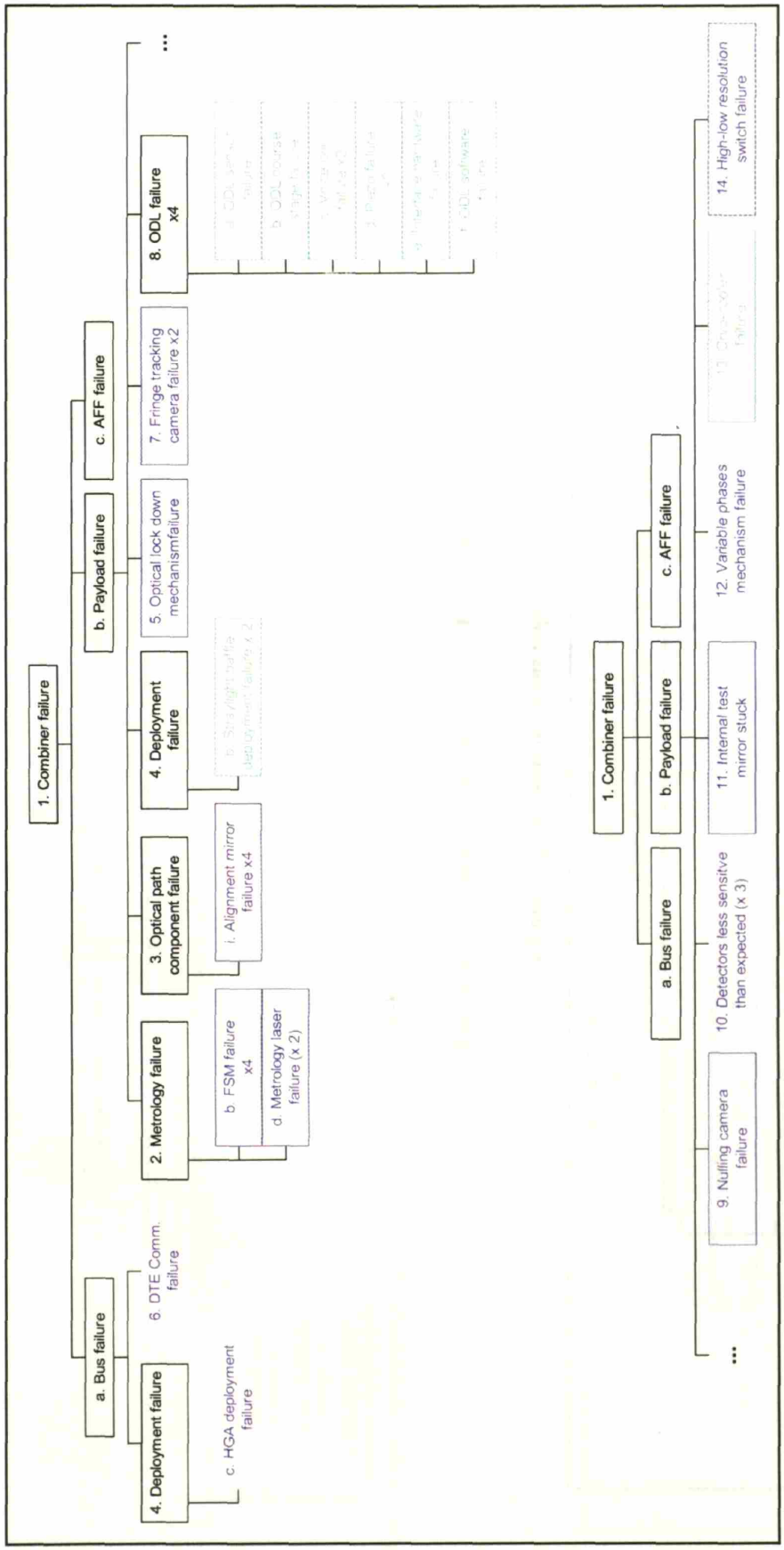


Figure A- 8: Failures specific to the combining spacecraft

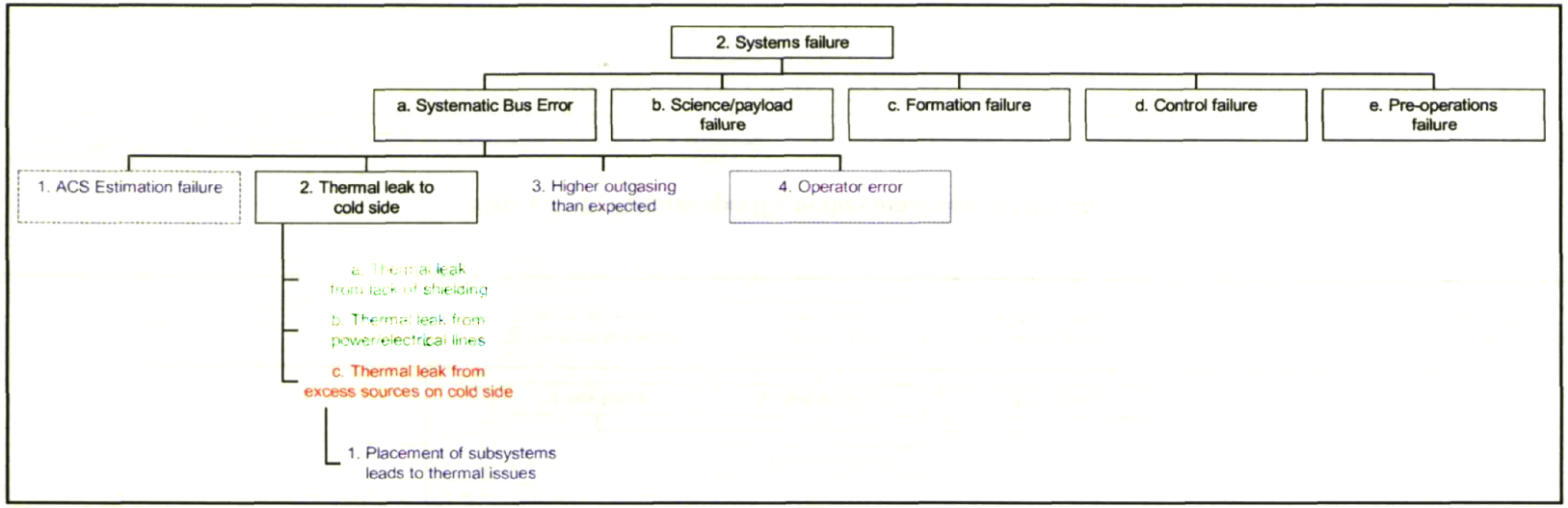


Figure A- 9: Systems level bus failures

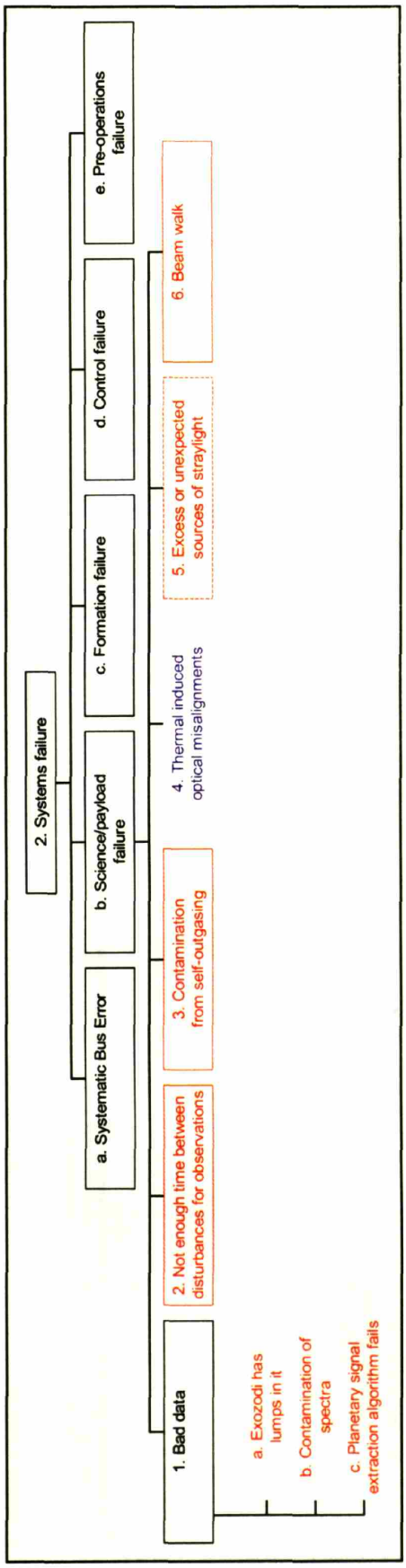


Figure A- 10: Systems level science or payload failures

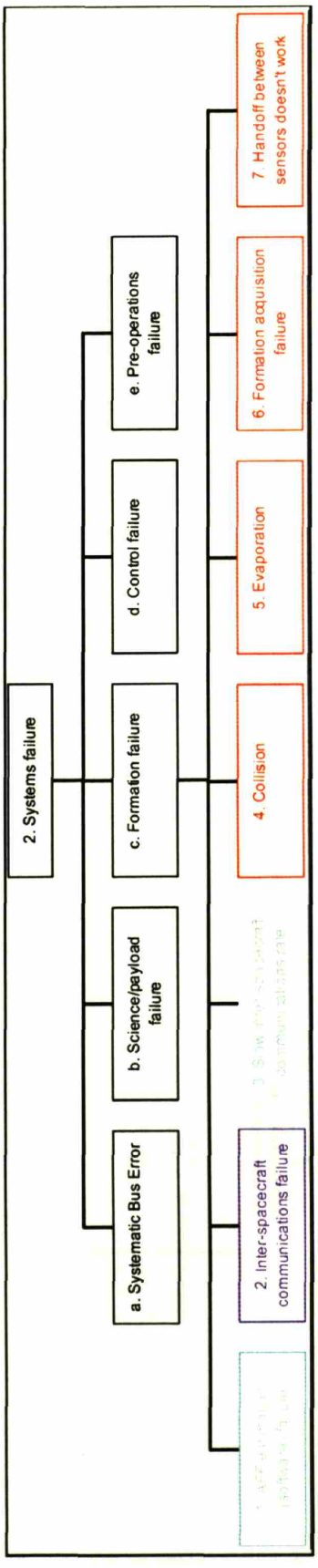


Figure A- 11: Systems level formation failures

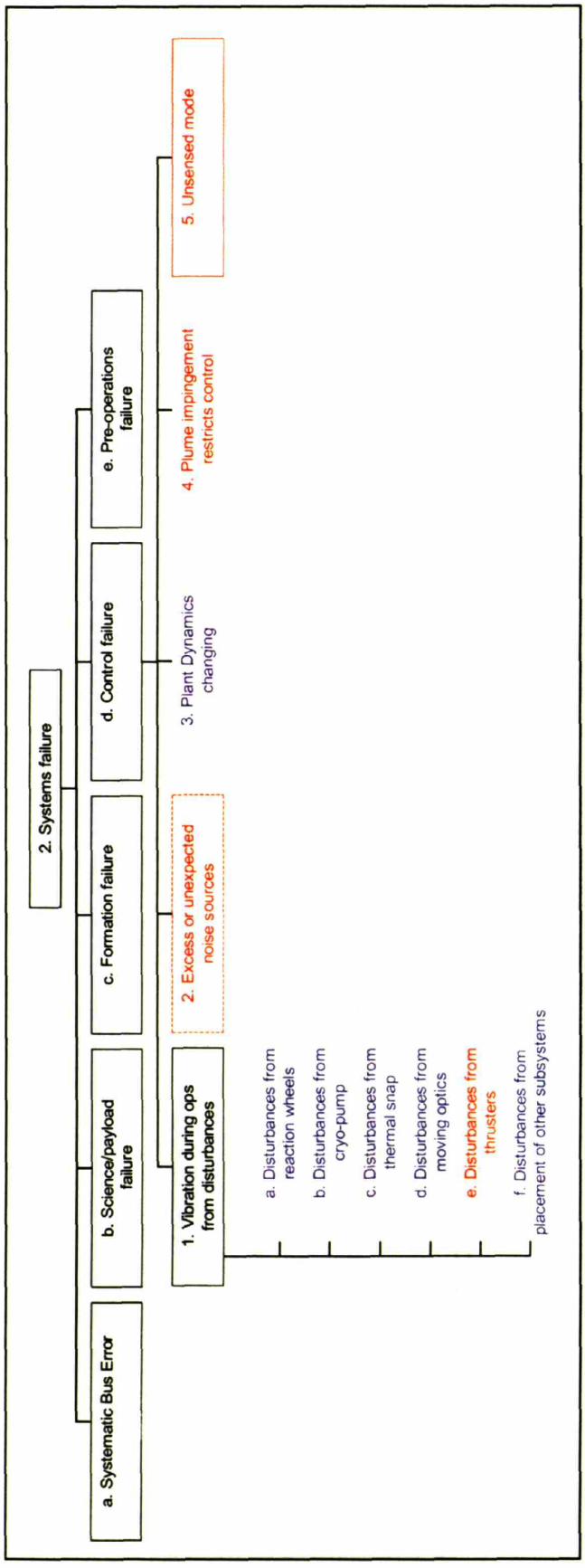


Figure A- 12: Systems level control failures

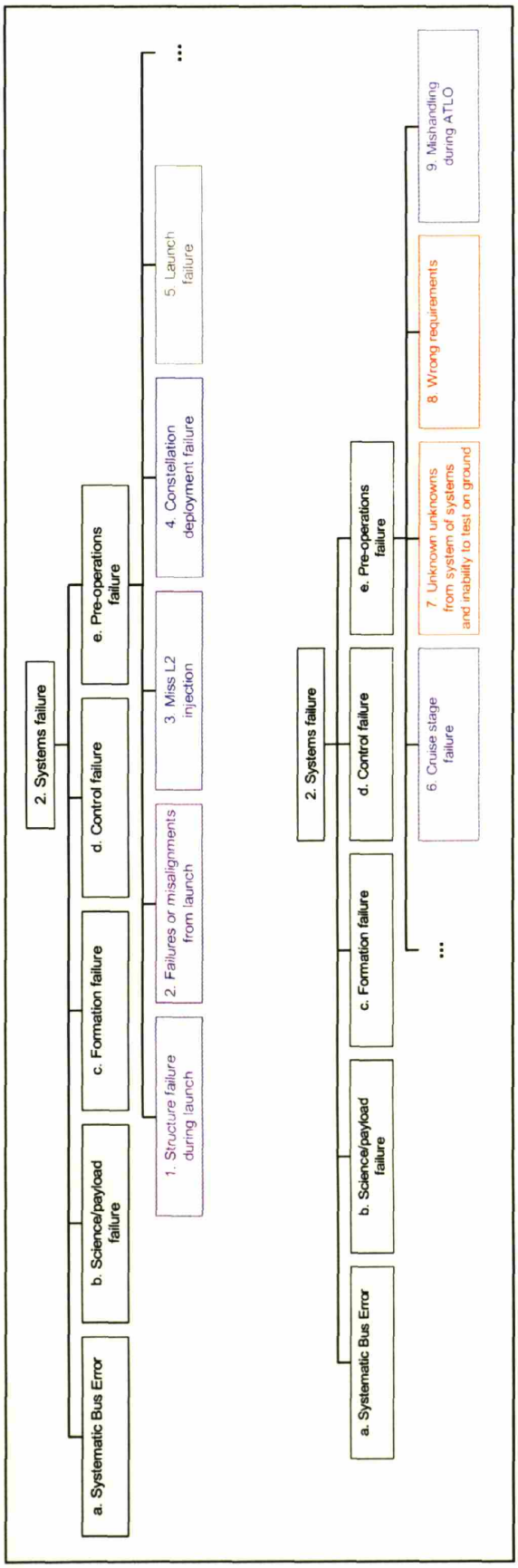


Figure A- 13: Systems level pre-operations failures

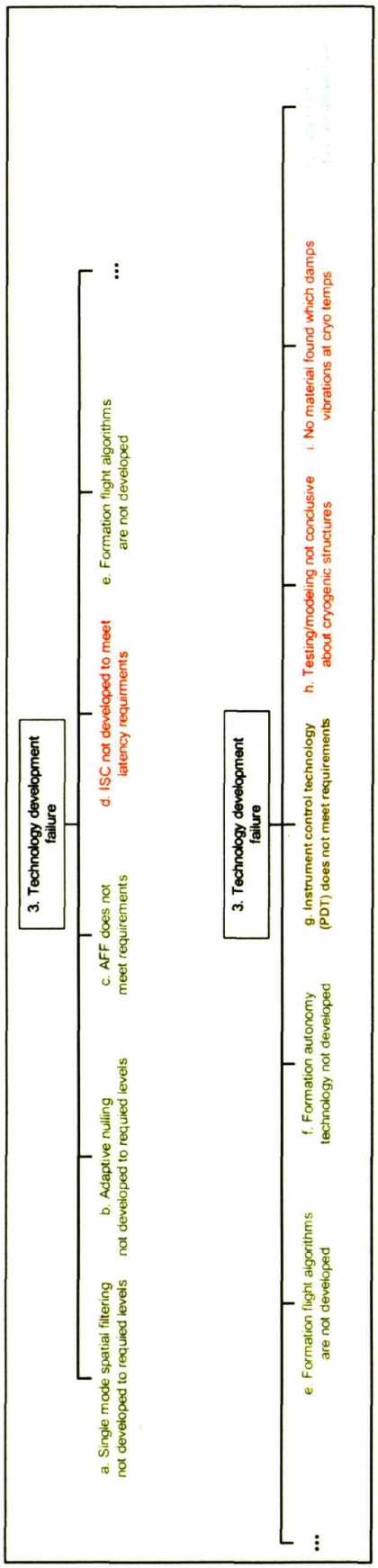


Figure A- 14: Technology development failures

7958-93