

INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI[®]

**Bell & Howell Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600**

**PROGRAMMATIC RISK ANALYSIS:
ENGINEERING AND MANAGEMENT RISK
TRADEOFFS FOR INTERDEPENDENT PROJECTS**

**A DISSERTATION
SUBMITTED TO THE DEPARTMENT OF INDUSTRIAL
ENGINEERING AND ENGINEERING MANAGEMENT
AND THE COMMITTEE ON GRADUATE STUDIES
OF STANFORD UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY
IN
INDUSTRIAL ENGINEERING**

Robin L. Dillon

June 1999

UMI Number: 9943643

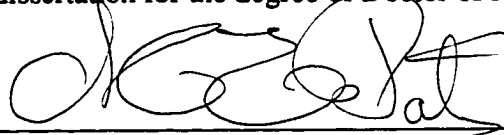
UMI Microform 9943643
Copyright 1999, by UMI Company. All rights reserved.

**This microform edition is protected against unauthorized
copying under Title 17, United States Code.**

UMI
300 North Zeeb Road
Ann Arbor, MI 48103

© Copyright by Robin L. Dillon 1999
All Rights Reserved

I certify that I have read this dissertation and that in my opinion it is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.



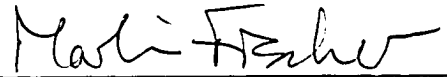
M. Elisabeth Paté-Cornell (Principal Advisor)

I certify that I have read this dissertation and that in my opinion it is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.



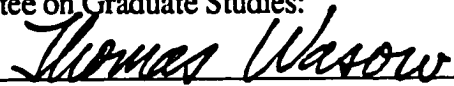
Margaret L. Brandeau

I certify that I have read this dissertation and that in my opinion it is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.



Martin A. Fischer

Approved for the University Committee on Graduate Studies:



ABSTRACT

Classical programmatic risk analysis focuses exclusively on budget and schedule. Yet, in the development of a critical system, the reliability also matters. The purpose of this dissertation is to develop a qualitative approach to tradeoff technical and management risks in interdependent projects within a program. Technical risks concern engineering failures. Management risks refer to schedule and budget overruns.

This research develops a probabilistic program risk management (PPRM) model involving a sequence of three optimization steps. The first step optimizes feasible technical design alternatives over the range of potential budgets to minimize each alternative's probability of technical failure. The second step considers the potential management risks associated with each design alternative and optimizes the risk mitigation strategy as a function of the budget reserve. The third step determines the optimal technical design alternative and budget reserves based on the lowest overall expected failure costs (or maximization of another utility function) considering both technical and management failures.

The presentation of the PPRM model is structured around a set of assumptions regarding problem detection, partial failures, and project dependencies. First, the model analyzes, for one project, the optimal selection of the design configuration, the choice of components, and the optimal reserve level. Second, the model considers the same decisions in conjunction with the optimal level of testing and reviews ("warning systems"). Third, the model considers the same decisions for one project, but includes partial failures. Finally, the model examines the management of one project when the outcome of this project affects other projects in the program. To check the effect of the budget constraint on the overall failure risk, we compute the shadow "risk cost" of the budget constraint, which is the variation of the failure risk of a project when the project resources vary by one unit. Illustrations of the model are based on a hypothetical case from NASA's unmanned space missions, which provides rich examples of dependent projects involving limited resources and multiple tradeoffs within programs.

The contribution of this dissertation is an analytical framework for (1) quantifying program risks (technical failures and management failures) to support management decisions about system design and financial reserves as a function of the budget, (2) explicitly comparing and trading off technical and management risks, and (3) modeling the effects of dependencies among projects in a program.

ACKNOWLEDGMENTS

I am very grateful to my advisor, Elisabeth Paté-Cornell, for her direction, support, and friendship throughout my years at Stanford. I came to Stanford to work with her, and I never regretted that decision. Without her help, none of this would have been possible.

I would like to thank the rest of my dissertation committee, Margaret Brandeau and Martin Fischer, for always finding some time for me. I would like to thank Maria Bharwada for her generous help, support, and supplies. I would also like to thank the people at the Jet Propulsion Laboratory for a challenging problem and several years of research support.

Finally, I would like to thank my family and friends for their endless support and encouragement. I needed a great deal of both through the years.

TABLE OF CONTENTS

CHAPTER 1: Introduction.....	1
1.1 Research Motivation	1
1.2 Problem Statement and Research Objective	4
1.3 Organization of the Dissertation	9
CHAPTER 2: Background and Related Research.....	11
2.1 Project Management.....	11
2.1.1 Empirical Studies of Projects.....	12
2.1.2 Project Management Tools.....	15
2.2 Analytical Modeling Tools for Systems	19
2.2.1 Decision Analysis.....	19
2.2.2 Probabilistic Risk Analysis	21
2.3 Mars Exploration Program	22
CHAPTER 3: Probabilistic Program Risk Management (PPRM) Model,	
Case 1- One Project	26
3.1 Introduction to the PPRM Model.....	26
3.2 PPRM Model Description for Case 1	28
3.3 Illustration of the Model for Case 1	34
3.4 Summary for Case 1	46
CHAPTER 4: Case 2- Single Project, Warning System Required for	
Problem Detection	47
4.1 Introduction to the PPRM Model with a Choice of a Warning System	47
4.2 Model Revisions to Include a Choice of Warning System	48
4.3 Illustration of the Model for Case 2	51
4.4 Summary for Case 2	64

CHAPTER 5: Case 3- Single Project with Partial Failures	65
5.1 Introduction to the PPRM Model with Partial Failures	65
5.2 Model Revisions to Include Partial Failures.....	65
5.3 Illustration of the Model for Case 3	68
5.4 Summary for Case 3	80
CHAPTER 6: Case 4- Dependent Projects in a Program.....	81
6.1 Introduction to the PPRM Model for Dependent Projects in a Program	81
6.2 Program Model Descriptions.....	82
6.3 Illustration of PPRM Model for a Program of Two Projects.....	83
6.4 Summary for Case 4.....	95
CHAPTER 7: Recommendations, Conclusions and Future Research.....	96
7.1 Research Summary.....	96
7.2 Conclusions and Recommendations for Structuring and Managing Programs of Projects.....	98
7.3 Limitations and Future Research Directions.....	100
REFERENCES	102

LIST OF TABLES

Table 3.1	Case 1: Probability of Failure Modes, Configuration 1	36
Table 3.2	Case 1: Effects of Investment on Reinforcement of Configuration 1	37
Table 3.3	Case 1: Probability of Failure Modes, Configuration 2	39
Table 3.4	Case 1: Effects of Investment on Reinforcement of Configuration 2	39
Table 3.5	Case 1: Management Risk Data for Configuration 1	41
Table 3.6	Case 1: Management Risk Data for Configuration 2	42
Table 3.7	Case 1: Design Alternatives for Configuration 1	44
Table 3.8	Case 1: Design Alternatives for Configuration 2	45
Table 3.9	Case 1: Shadow Cost of Budget Constraint	46
Table 4.1	Case 2: Design Alternatives for Configuration 1, WS_1	52
Table 4.2	Case 2: Design Alternatives for Configuration 2, WS_1	52
Table 4.3	Case 2: Probability of Failure Modes Given No Undetected Problems, Configuration 1, WS_2	54
Table 4.4	Case 2: Probability of Failure Modes Given Undetected Problems, Configuration 1, WS_2	54
Table 4.5	Case 2: Probability of Undetected Problems, Configuration 1, WS_2	54
Table 4.6	Case 2: Effects of Investment on Reinforcement of Configuration 1, WS_2	55
Table 4.7	Case 2: Probability of Failure Modes Given No Undetected Problems, Configuration 2, WS_2	57
Table 4.8	Case 2: Probability of Failure Modes Given Undetected Problems, Configuration 2, WS_2	57
Table 4.9	Case 2: Probability of Undetected Problems, Configuration 2, WS_2	58
Table 4.10	Case 2: Effects of Investment on Reinforcement of Configuration 2, WS_2	58
Table 4.11	Case 2: Management Risk Data for Configuration 1, WS_2	60
Table 4.12	Case 2: Management Risk Data for Configuration 2, WS_2	61
Table 4.13	Case 2: Design Alternatives for Configuration 1, WS_2	63
Table 4.14	Case 2: Design Alternatives for Configuration 2, WS_2	63

Table 5.1	Case 3: Probability of Failure Modes, Configuration 1, WS_1	70
Table 5.2	Case 3: Effects of Investment on Reinforcement of Configuration 1, WS_1	71
Table 5.3	Case 3: Management Risk Data for Configuration 1, WS_1	76
Table 5.4	Case 3: Management Risk Data for Configuration 2, WS_1	77
Table 5.5	Case 3: Design Alternatives for Configuration 1, WS_1	79
Table 5.6	Case 3: Design Alternatives for Configuration 2, WS_1	79
Table 6.1	Case 4: Probability of Failure Modes, Project 2, Configuration 1.....	85
Table 6.2	Case 4: Effects of Investment on Reinforcement of Project 2, Configuration 1.....	85
Table 6.3	Case 4: Probability of Failure Modes, Project 2, Configuration 2.....	87
Table 6.4	Case 4: Effects of Investment on Reinforcement of Project 2, Configuration 2.....	87
Table 6.5	Case 4: Management Risk Data for Project 2 (Assuming No Failure in Project 1).....	89
Table 6.6	Case 4: Optimal Technical Design Alternatives for Project 2 Conditional on the Outcome State of Project 1	91
Table 6.7	Case 4: Design Alternatives for Project 1, Configuration 1, WS_1 with Additional Program Penalties.....	92
Table 6.8	Case 4: Design Alternatives for Project 1, Configuration 2, WS_1 with Additional Program Penalties.....	93
Table 6.9	Design Alternatives for Project 1, Configuration 1, WS_1 with Large Program Penalties for Technical Failure.....	94
Table 6.10	Design Alternatives for Project 1, Configuration 2, WS_1 with Large Program Penalties for Technical Failure.....	94

LIST OF FIGURES

Figure 1.1	Risk Elements for a Project.....	5
Figure 1.2	Cases for the PPRM Model.....	7
Figure 3.1	Risk Components and PPRM Steps.....	26
Figure 3.2	Case 1: Budget Allocation Between Development and Reserves.....	27
Figure 3.3	One Possible Functional Configuration (FIG_z).....	29
Figure 3.4	Lowest Cost Alternative for Configuration z ($AFIG_{z,min}$)	30
Figure 3.5	Example Decision Tree.....	32
Figure 3.6	Summary of Optimization Algorithm.....	34
Figure 3.7	Case 1: Spacecraft Functional Block Diagram.....	34
Figure 3.8	Case 1: Single-string design, $z = 1$	35
Figure 3.9	Case 1: Spacecraft with Redundant Communications System, $z = 2$	35
Figure 3.10	Case 1: Various Investment Levels for Configuration 1	38
Figure 3.11	Case 1: Various Investment Levels for Configuration 2	40
Figure 3.12	Case 1: Portion of the Decision Tree for Configuration 1.....	42
Figure 3.13	Case 1: Probability of Management Failure as a Function of the Reserve Allocation for Configurations 1 and 2	43
Figure 4.1	Case 2: Budget Allocation Between Development, Warning System, and Reserves.....	48
Figure 4.2	Case 2: Various Investment Levels for Configuration 1, WS_2	56
Figure 4.3	Case 2: Various Investment Levels for Configuration 2, WS_2	59
Figure 4.4	Case 2: Portion of the Decision Tree for Configuration 1, WS_2	61
Figure 4.5	Case 2: Probability of Management Failure as a Function of the Reserve Allocation for Configurations 1 and 2, WS_2	62
Figure 5.1	Case 3: Example Decision Tree with Partial Management Failures	67
Figure 5.2	Possible Outcome States Including Partial Failures.....	68
Figure 5.3	Case 3: Instrument Package	70
Figure 5.4	Case 3: Various Investment Levels for Configuration 1, WS_1	72
Figure 5.5	Case 3: Probability of Failure States for Various Investment Levels for Configuration 1, WS_1	73
Figure 5.6	Case 3: Various Investment Levels for Configuration 2, WS_1	74

Figure 5.7	Case 3: Probability of Failure States for Various Investment Levels for Configuration 2, WS_1	75
Figure 5.8	Case 3: Probability of Management and Partial Management Failure as a Function of the Reserve Allocation for Configurations 1 and 2, WS_1	78
Figure 6.1	Case 4: Management Decisions for Dependent Projects in a Program.....	81
Figure 6.2	Case 4: Project 2 Spacecraft Functional Block Diagram	83
Figure 6.3	Case 4: Project 2, Single-string design, $z = 1$	83
Figure 6.4	Case 4: Project 2, Spacecraft with Redundant Communications System, $z = 2$	83
Figure 6.5	Case 4: Various Investment Levels for Project 2, Configuration 1	86
Figure 6.6	Case 4: Various Investment Levels for Project 2, Configuration 2	88
Figure 6.7	Case 4: Probability of Management Failure for Project 2 as a Function of the Reserve Allocation and the Failure Scenario of Project 1	90

CHAPTER 1

Introduction

1.1 Research Motivation

Many complex engineering programs have experienced substantial budget or schedule overruns in the development phase, or catastrophic failures in the operational phase. In some cases, the problems arise from a large number of interdependent components that must all come together in a final project. Also, in many cases, problems occur because the project development team is tightly constrained for resources and must make difficult tradeoffs among the competing risk elements (cost, schedule, and technical performance). Two of many possible examples include the space shuttle Challenger project and the development of the international space station. In the case of the Challenger, a technical failure resulted in the loss of human life. In the case of the space station, management failures have resulted in long delays and cost overruns, and future technical failures could result in loss of life. The key issue in developing these complex programs is to appropriately manage the available development resources to minimize the probability of technical failure as well as cost and schedule overruns. This dissertation provides a modeling framework to support these management decisions.

On January 28, 1986, the space shuttle Challenger exploded seconds into its flight, killing all six astronauts on-board. Following the accident, the history of the NASA shuttle program was scrutinized by many independent review boards. The cause of the accident, the failure of the solid rocket booster joint, was determined to be the result of a faulty design. The reviews also showed that some engineers knew of this inadequate design since 1977 [Pinkus, et al., 1997], and some recommended against launch in the extremely low temperatures predicted for that day. Many studies have highlighted reasons for the poor decision to launch, including poor communications among the engineers and the decision makers as well as a success-oriented management philosophy. Pinkus, et al. [1997], however, concludes, "The disaster...was not a single event. Rather, the decision by Congress to fund the space shuttle program at a 'cut-rate' price and the acceptance by NASA to proceed with plans to build the shuttle set the stage for individual engineers continually to struggle to balance safety, cost, and timing."

The development of the international space station (ISS) includes ten major modules, requires significant technology development, and needs the cooperation of sixteen

countries. In 1994, NASA claimed that the ISS could be completed for \$2.1 billion per year (total cost: \$17.4 billion). Many managers at NASA hoped that Russian technology in the ISS Program would accelerate the assembly timetable and minimize substantial development costs in the areas of propulsion and navigation. A NASA review board evaluated the situation differently: "NASA's cost and schedule plans have been optimistic from the beginning of the Program and continue to be so today. Budget and reserve levels have been, and continue to be, inadequate for a program of this size, complexity, and development uncertainty despite NASA's past contentions that the total funding level is adequate. It could alternatively be stated that the Program has more content than it has funds available to achieve...The Program should plan for the development schedule to extend an additional two years with additional funding requirements of between \$130 million and \$250 million annually...This level of funding and schedule extension results in a total assessed cost of approximately \$24.7 billion from the 1994 ISS redesign through ISS Assembly Complete" [NASA Advisory Council, 1998].

Despite the complexity and risks associated with major programs, organizations increasingly have adopted a "faster-better-cheaper" (FBC) mode of management, in which both schedules and budgets are strictly set. When these programs include the development of new technology, the risks are even greater because of the difficulties in achieving technological breakthroughs within tight budget and schedule constraints. Managing programs successfully in this environment depends on the manager's understanding of cost, schedule, and performance uncertainties, as well as major risks affecting the overall program. Quantitative risk estimates of the competing elements (cost, schedule, and technical performance) are useful in supporting management decisions because the estimates allow the managers to explicitly examine the risk tradeoffs.

Currently, risk modeling tools focus on quantifying either the technical risk or the management (cost or schedule) risk. Probabilistic risk analysis (PRA) has been used successfully in evaluating the technical risks in specific projects, (i.e., for the NASA Cassini mission, the risk of radiological exposure from a catastrophic accident). Traditionally, this approach is used to support design decisions to minimize the probability of a technical failure of the system. Attempts have been made to include uncertainty when examining the risks of cost escalation or schedule slippage for a project [Williams, 1995]. These risk analysis tools while beneficial, are too often used in isolation. Suppose that the project team completes a risk analysis of the cost of the project and determines that there is only a probability of 0.5 of meeting the budget constraint. This result does not indicate that

the project will overrun its budget, but that there exists a non-zero probability that actions will need to be taken to reduce the cost. These actions may have schedule or performance implications. Since it is a difficult task to simultaneously balance project cost, schedule, and performance, and the dependencies among the project risks, managers who face these problems can benefit from an integrated probabilistic risk analysis approach.

Some risk analysis techniques have been previously proposed to integrate cost, schedule, and performance risk [Kidd, 1987 and Weist, 1985]. These methods, however, are only useful for analyzing potential project outcomes, primarily cost or duration, (i.e., if problems *a* and *b* occur, what would the project's expected life-cycle cost or expected development duration). Performance is defined in terms of a measurable outcome unit (e.g., quantity of items produced). It is not the probability of failure. Also, because the methods are based on a Program Evaluation and Review Technique (PERT) activity network, quantifying the cost, schedule, and contribution to performance for each activity in the network becomes quantitatively cumbersome and can require somewhat unrealistic estimates of performance or quality. For this reason, a model that includes both technical and management risks for programs of projects can be an important contribution.

To examine program risk management, one could use an empirical approach, studying a sample of organizations and examining how, in the past, programs have been successfully managed [Jaselskis and Ashley, 1991, and RAND, 1988]. These empirical models use databases of projects and apply regression models to correlate descriptive factors with the likelihood of project success. For example, a RAND [1988] study used project characteristics such as type of project, project location, and project ownership to predict cost growth and schedule slippage. Most complex engineering programs, however, involve unique systems. Thus, statistical relationships of significant project characteristics based on past experience may only be partially relevant.

This dissertation develops an analytical model, the Probabilistic Program Risk Management (PPRM) model, for improving program and project management decision making processes. The PPRM model supports management decisions by quantifying: (1) the tradeoffs among the technical and management risks, (2) a decision maker's preference function for project outcomes that includes both managerial and technical success, and (3) the effects of dependencies among projects in a program. The PPRM model is intended to improve both the design process for the physical system and the management of the budget reserves.

1.2 Problem Statement and Research Objective

The purpose of this dissertation is to develop an approach for quantifying both technical and management risks in projects and across programs in order to manage the tradeoffs between the risks. As defined here, a project is a complex effort that begins and ends with a well-defined objective, schedule, and budget, while a program is a long-term undertaking that is made up of several, dependent projects, working toward a common, broader set of objectives.

Engineering risks are those factors that can lead to technical failure. Technical failures generally occur during operations when the project does not perform its functions. The primary cause of technical failures are flaws that were introduced during the design and development phase of the project and were not detected prior to operations. Human and organizational factors often contribute to system failures. For example, in the Lewis spacecraft which was lost three days after launch in 1997, the attitude control system failed to operate properly and caused the spacecraft to rotate to an incorrect alignment with the sun. This error was compounded by a project team that was not adequately monitoring the spacecraft during the initial mission phase. The team did not detect the incorrect alignment of the solar arrays until the batteries had depleted, and the mission was lost.

Management risks focus on factors that affect the schedule and the budget of a project. Many projects have “failed” (i.e., were canceled) because large cost or schedule overruns caused either problems in the program management or in the way the constraints were set [RAND, 1988]. Failures of this type are considered management failures.

For the complex engineering systems examined in this dissertation, the problem is to consider simultaneously both the management and technical risks and the tradeoffs that exist between them. For example, if the development team “cuts corners” on costs by procuring cheaper parts, these choices may increase the probability of technical failure for the system. Similarly, if the team decides to reduce the schedule duration and chooses to eliminate either some reviews or some tests, these actions could also increase the probability of system failure. The challenge for managers is to consider all risk factors and understand which tradeoffs among the different risk components are acceptable for the program. Figure 1.1 shows the risk elements for a single project in a hierarchy. For a program, the risk elements include the technical and management failure risks for each project. In this dissertation, the failure risks are simply measured by the expected value of the failure cost, independently from the mission value. Current research to develop a

measure for the value of a mission is beyond the scope of this dissertation [Reiter, et. al., 1999].

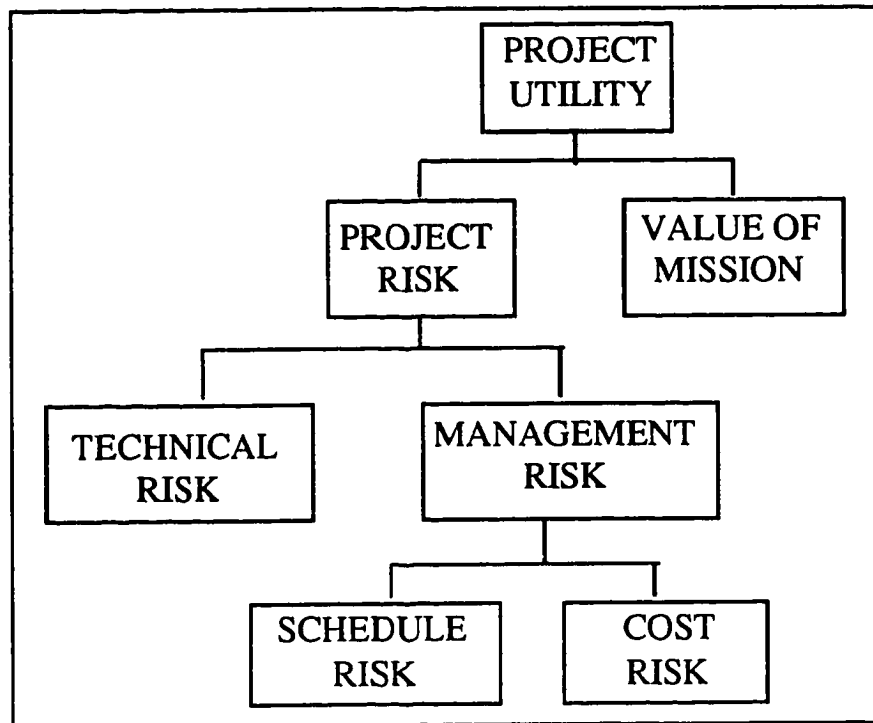


Figure 1.1- Risk Elements for a Project

Managers affect the success or failure of a program or project through their decisions, and the PPRM model supports these management decisions. Each project is successful if it meets its specified objectives, and successful projects contribute to the achievement of program objectives. Some of the success-critical decisions for a project include:

- What fraction of the budget should be allocated to reserves? Reserves refer to the resources held separately for the express purpose of accommodating mistakes and oversights and resolving development problems.
- How to spend the project development budget to maximize technical reliability? This includes: what fraction to allocate to risk analysis and what fraction to allocate to testing and reviews?
- How much of a project's schedule should be held in reserve to cover potential project delays?

- How to spend the reserves to maximize technical reliability and minimize the potential for management failures?

The PPRM model provides decision support to the project manager in answering these questions. It is structured into three sequential optimization steps:

STEP 1: Develop and optimize all feasible technical design alternatives over the range of potential project development budgets to minimize each alternative's probability of technical failure.

STEP 2: For each technical design alternative, optimize the strategy to reduce management risks over the range of potential reserve budgets, where the strategy is determined by:

- the potential management problems that could occur for each technical design alternative, and
- potential mitigation actions for each management problem.

STEP 3: Determine the optimal technical design alternative and budget reserve based on the lowest overall expected failure cost given the optimal management risk strategies for that design.

The implementation of this optimization algorithm is examined for a series of cases. Figure 1.2 shows the different cases considered in this dissertation. In Case 1, a fixed project budget is optimally allocated between the project development budget and the reserves with a portion of the development budget required for risk analysis. These allocation decisions directly affect the probabilities of different types of failure for the mission. For example, allocating more money to the development budget (and less to reserves), may increase the technical reliability of the mission. Failure to maintain sufficient reserves, however, could critically affect the project should unforeseen problems occur. In Case 1, the assumption is made that as soon as problems occur during development, they are detected. Therefore, the resources needed for testing and reviews are implicit in the development costs.

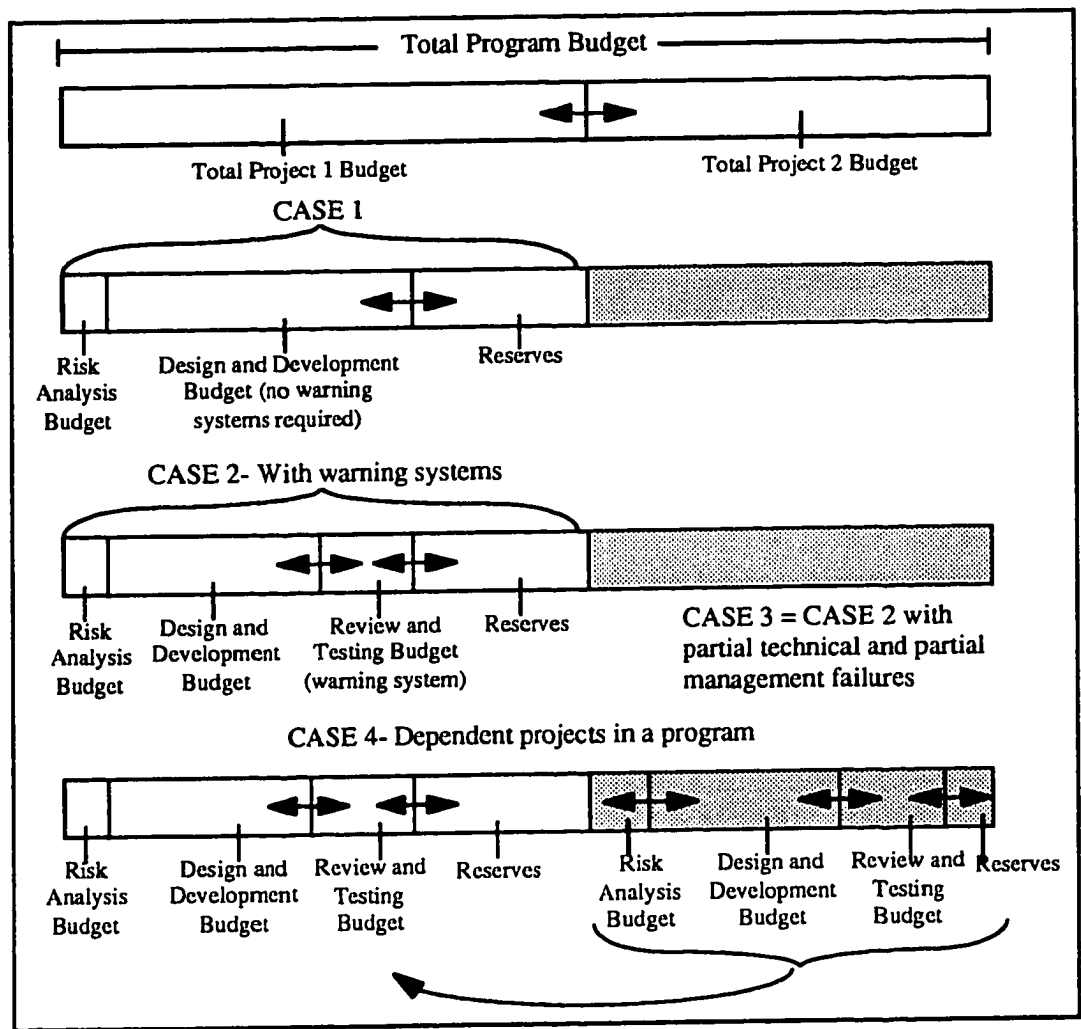


Figure 1.2- Cases for the PPRM Model

In Case 2, the assumption of problem detection is relaxed and warning systems are required to detect problems during development. The amount of project budget allocated to reviews and testing affects the chances that development problems are detected and corrected, and therefore influences the probabilities of technical and management failures.

Case 3 expands Case 2 by including partial project failures. If problems occur in a component requiring technology development, this component can sometimes be "descoped," thus resulting in partial project management failure. Also, depending on the configuration of the system, a portion of the project can fail without total loss of the mission. This result is classified as a partial technical failure.

In Case 4, a program of two projects is analyzed. In programs, the results of earlier projects can influence the development and success of subsequent projects. Case 4 examines the optimal allocation of project 1 resources while considering the impact of the possible outcomes of project 1 on project 2. For example, a potentially risky technical design alternative may be acceptable as an independent project. If, however, a future project is relying on a successful outcome for that project, then a more robust design may be preferable. The ability to shift resource among projects is not considered here and is part of potential future work.

The illustrations presented in this dissertation are based on NASA's unmanned space program. In an attempt to reduce the complexity of a project, and therefore, the risks associated with it, NASA has adopted a faster-better-cheaper mode of management for its unmanned space missions. Current projects have reduced scopes (compared to previous projects) and are developed in three-year time frames for approximately two hundred million dollars. The focus is on more numerous and smaller spacecraft that remove the risk of losing one big "flagship" project (i.e., don't put all the "eggs in one basket"). The NASA unmanned space program provides rich examples of projects involving limited resources and many tradeoffs within programs. The illustrations in this dissertation are designed to demonstrate the applicability and practicality of this research.

For any analysis, the benefits must exceed the costs. The PPRM model as described in this dissertation uses a technical probabilistic risk analysis (PRA) model and additional analysis of the potential management risks. Project managers need to consider the best technical design alternative that could be developed without the PPRM model and compare this design to the computed optimal. The PPRM model has value for the project if the savings in the expected failure costs of the optimal technical design alternative are greater than the cost of the analysis.

In conclusion, the problems faced by complex development programs are not new. In reference to the Polaris Fleet Ballistic Missile Program of the 1950's, Sapolsky [1972] wrote: "The greatest uncertainty in the project becomes the political uncertainty over its own future. To both the observer and participant, the research and development issue looks inefficient; there are likely to be cost overruns because of underbidding, schedule delays because of irregular funding, and inadequate technical performance because of a failure to gain a concentrated effort." While the problem may not be new, the approach to modeling and analyzing complex development programs described in this dissertation, however, is

new. The PPRM model explicitly quantifies both the management and technical risks and the tradeoffs between them for a project while evaluating the potential impact of that project on a program.

1.3 Organization of the Dissertation

The remainder of this dissertation is organized as follows. Chapter 2 provides an introduction to the literature that is related to the problem and research described in this dissertation. The literature survey focuses on three areas: the current state of the art in project and program management, systems analysis tools relevant to the research approach, and an example of program management. In reviewing project management research, both empirical studies of past projects and the analytical tools of project management are examined. The systems analysis tools necessary for this research are decision analysis and probabilistic risk analysis. The program management example is NASA's Mars Exploration Program. This program is the basis for illustrative examples for the research model described in this dissertation and demonstrates some of the risks facing real programs.

Chapter 3 describes the framework for the PPRM model and examines the simplest case, Case 1. Case 1 includes only one project, and problems are immediately detected when they occur (testing and reviews are implicit in the development phase, and there are no undetected problems in the system). The outputs of the PPRM model for Case 1 are (1) the recommended functional design configuration and choice of components, and (2) the development budget and corresponding reserve budget.

Chapter 4 describes the use of the PPRM model in determining the appropriate level of "warning system" (reviews and testing). In Case 2, problems are not automatically detected, and a warning system while helpful is imperfect in detecting problems. Allocating more resources to the warning system increases the detection capability. These resources, however, are then not available for project development or for reserves. The outputs of the PPRM model for Case 2 are (1) the recommended functional design configuration and components, (2) the development budget and corresponding reserve budget, and (3) the recommended choice of warning system (level of testing and frequency and depth of reviews).

Chapter 5 describes the expanded PPRM model where the project in addition to requiring some level of warning system for detecting problems, can also fail *partially*. A partial management failure occurs when the managers decide to reduce the scope of the mission in order to remain within the cost and schedule allocations ("descope"). The potential for a descope is often associated with the development of new technology. A partial technical failure occurs if the project completes only a portion of its mission (e.g., only one of three instruments functions properly). The outputs of the PPRM model are the same as for Case 2, except that the recommendations in addition include the effects of partial failures.

Chapter 6 describes Case 4, the management of a project within a program. The management of the first project must consider the effects of potential project problems and management actions on future projects. The modeling approach first considers the impact of a failure of project 1 in the optimization of project 2. The additional costs to project 2 that result from a failure in project 1 are then included in the optimization process for project 1. The outputs of the PPRM model for Case 4 are (1) the recommended functional design configuration and components for both projects, and (2) the development budget and corresponding reserve budget for each project.

The dissertation concludes with Chapter 7 which summarizes key contributions of this research, discusses some of its limitations, and suggests possible areas of future research. Chapter 7 also describes general recommendations for managing projects and programs and the benefits of using the PPRM model.

CHAPTER 2

Background and Related Research

The following sections introduce the major background topics relevant to this research. The first section describes the project management discipline, several empirical studies performed on databases of major projects, and the classical tools of project management. The second section discusses analytical modeling tools for analyzing systems, focusing specifically on the methods of decision and risk analysis. The third section briefly discusses NASA's Mars Exploration Program. This program is the basis for illustrative examples of the modeling approach described in this dissertation.

2.1 Project Management

Project management as a discipline formally started in the 1950s in part because of the need to develop and implement a philosophy for the management of new, complex military systems. The Project Management Institute defines project management as the art of directing and coordinating human and material resources throughout the life of a project using modern management techniques to achieve predetermined objectives of scope, cost, time, quality, and participant satisfaction [Cleland, 1994]. One of the first project management offices ever formed was the Special Projects Office for the Polaris Fleet Ballistic Missile program in 1955. This office was responsible for the development of the PERT method. By the early 1970s, professional societies for project managers had been established in Europe and the US. Since then there have been thousands of articles written on project management with recommendations for managing projects effectively [see, for example, Morris, 1986].

Project management articles focus primarily on the effective planning, control, and leadership of projects and programs. Two major categories of topics exist: (1) empirical studies that examine past projects to identify statistical relationships between project characteristics and the likelihood of project success, and (2) the development of analytical tools to assist in the management of projects.

Section 2.1.1 describes two major studies from the construction industry that examine databases of past projects to identify characteristics of projects that contribute either positively or negatively to the likelihood of project success. This description is intended

only to demonstrate the empirical approach to examining project management and is not a complete survey of all of the studies in this area of research.

Section 2.1.2 examines project management tools. The tools that are described are separated into deterministic and probabilistic techniques. In the first part of this section, we describe two deterministic management tools: work break-down structures (WBS) and activity networks [Bubushait, 1986]. In the second part, we introduce the current project management methods for cost risk analysis, schedule risk analysis, and some integrated risk analysis approaches. We conclude with a discussion of some of the limitations of these methods.

2.1.1 Empirical Studies of Projects

In this section, I discuss two empirical studies that analyzed databases of construction projects to determine important factors for predicting project performance. This discussion is not a comprehensive review of all of the studies of this type, but rather a descriptive summary of two studies meant to illustrate this type of research method. While this research method is interesting and may provide insight into the management of engineering programs, since most complex programs involve some unique systems, statistical relationships of significant project characteristics based on past experience may only be partially relevant. The research approach developed in this dissertation is different from the empirical method. It is based on a probabilistic risk analysis of the physical system to generate and evaluate management options specifically tailored to the project and its environment.

The RAND Corporation Study of Megaprojects

From late in the 1970s through 1988, the RAND Corporation performed a series of studies that examined very large projects (greater than \$500 million) to present useful recommendations for managers of future similar endeavors [RAND, 1988, RAND, 1981, and RAND, 1979]. In the final study [RAND, 1988], the authors examined 52 civilian construction projects with an average cost of \$2 billion and an average construction schedule of four years. Most of the projects examined met their performance goals. Many met their schedule goals, but very few met their cost goals. The average cost growth of the projects examined was 88%.

The authors used project factors and three multiple regression models to develop formulas for predicting cost growth, schedule slippage, and project performance. Of the factors considered, the regression models showed linear statistical relationships among:

- (1) cost growth and the number of regulatory problems encountered, the type of project ownership, the level of innovation in new materials or construction methods, the amount of first-of-a-kind technology used, and amount of infrastructure (permanent or temporary) at the site.
- (2) schedule slippage and the number of regulatory problems encountered, the amount of first-of-a-kind technology used, the level of innovation in new materials or construction methods, the type of project (i.e., if it is a minerals-extraction project), and the quantity of labor shortages that occurred during construction.
- (3) project performance and the level of innovation in new materials or construction methods, the amount of first-of-a-kind technology used, and whether or not the project was the largest project of its type ever constructed.

The study was useful in highlighting the importance of regulatory problems and new technologies in project development. Recommendations to reduce project risk included: (1) thoroughly understanding the institutional problems relating to regulations and labor practices, and (2) questioning whether the introduction of new technology, construction techniques, or design approaches is absolutely essential to the project. These same issues are also highlighted by the analytical systems approach developed in this dissertation.

Study of Construction Projects: Jaselskis and Ashley [1991]

Jaselskis and Ashley [1991] examined a database of 75 construction projects to develop linear regression models to predict the probability of success for future construction projects based on the management resources available to that project. All projects in the database were large multi-million dollar projects with at least 12,000 construction man-hours.

The authors used project factors and regression models to develop formulas for predicting the probability that the overall project is considered outstanding by all major participants, that the project experiences better-than-expected schedule performance, and that the project experiences better-than-expected cost performance. Of the factors considered, in predicting overall project success, five factors were considered significant:

- whether or not the project manager was the owner or a contractor,

- the percentage of team turnover per year,
- the level of dependency to other projects (i.e., the percentage of a program that the project comprised),
- the number of subordinates to the project manager on the project, and
- the number of project control (i.e., status and tracking) meetings held per month during construction.

In predicting the probability of better-than-expected schedule performance, five factors were considered significant:

- the contract type (fixed price or reimbursable cost),
- the number of years of education after high school of the project manager,
- the level of dependency to other projects (i.e., the percentage of a program that the project comprised),
- the percentage of team turnover per year, and
- the number of budget updates per year.

In predicting the probability of better-than-expected budget performance, six factors were considered significant:

- the percentage of the overall budget allocated to project control (i.e., status and tracking) activities,
- the number of project control (i.e., status and tracking) meetings held per month during design,
- the number of project control (i.e., status and tracking) meetings held per month during construction,
- the number of budget updates per year,
- the percentage of team turnover per year, and
- the technical experience of the project manager as measured by the number of previous projects developed with similar technology.

From the authors' analysis, the models appear to perform reasonably well in predicting outstanding project performance. The models are also useful in analyzing the impact of specific factors, (e.g., team turnover, budget updates, etc.), on project performance. As with the first study, several of the factors highlighted by the regression models are also

important in the analytical model developed in this dissertation, specifically, the level of dependency to other projects and the percentage of the overall budget allocated to project control.

2.1.2 Project Management Tools

Research in the discipline of project management has also focused on the development of analytical tools to effectively plan, control, and lead projects and programs. These tools are designed, however, to handle only management problems and do not include the potential risk tradeoffs between these problems and technical failure risks. These tools are categorized into deterministic and probabilistic methods.

Deterministic Project Management Tools

Work break-down structures (WBS): The development of the WBS begins at the highest level of the program with the identification of major components. The component parts are further divided and subdivided into more detailed units with each division reducing the dollar value and the complexity of the units. This process is repeated until the WBS reaches a level where the component parts are at manageable levels for planning and control purposes. The end items appearing at the lowest level are usually considered work packages. The term work package is a general term used to identify discrete tasks with definable end results. The responsibility of completing a work package on schedule and within budget is assigned to an organizational unit. Project managers then track the status of the work packages by who is responsible for what and when [Cleland, 1994, and Moder, et al., 1983]. The NASA Jet Propulsion Laboratory has incorporated the WBS structure into an information system to formalize, maintain, and track all receivables and deliverables between the elements of a program, and the dependencies among the packages. By tracking and continually updating who owes work packages to whom, the system can provide an accurate project status report and also analyze the program impacts of late work package deliveries.

Activity networks or bar (Gantt) charts: A schedule is an expression of tasks and activities to be performed along a time-line. The two main methods for describing a schedule are (1) PERT/CPM (Project Evaluation and Review Technique/Critical Path Method) charts where activity dependencies are displayed graphically in an activity network and (2) Gantt charts where the dependencies are displayed in a bar chart format. CPM is a schedule activity network that assumes that each activity has a known deterministic schedule length. PERT

models are the simplest project activity planning models that consider risk because PERT networks include probability distributions for each activity duration [Eisner, 1997, and Chapman and Ward, 1997]. Details of a stochastic PERT analysis are described below in the discussion of schedule risk analysis models.

In summary, these deterministic tools are primarily useful for project status reporting. The project WBS and activity networks are helpful initially in project planning and scheduling, and later for tracking cost, schedule, work performed, and work remaining. In order to manage risks, however, problems and their associated probabilities are required. Deterministic tools can provide the organizing structure to analyze project risks when probabilities are incorporated.

Probabilistic Project Management Tools

Project management has recognized that a project's performance can be improved by systematically identifying, appraising, and managing the project's risks. Standard tools exist for including uncertainty in cost and schedule estimates, and some models have been developed that attempt to integrate these uncertainties with some basic measures of performance such as quantity of items produced.

Cost risk analysis

Cost risk analysis models attempt to estimate the likelihood of not meeting cost estimates. Research has shown that the primary causes of cost problems are [Archibald, 1992]:

- unrealistic, low original estimates, bids, and budgets,
- a management decision to reduce bid price to meet competitive pressures,
- uncontrolled increases in scope of work,
- unforeseen technical difficulties,
- schedule delays that require overtime or added cost to recover from the delays or the charging of idle labor time to the project during the delays, and
- inadequate cost budgeting, reporting, and control practices and procedures.

As early as the 1960s, project managers realized that cost estimates needed to include probabilistic information [Hertz, 1964]. The traditional approach to cost estimating was to derive a best estimate from the current knowledge and add a contingency factor to cover unforeseen expenditures. The size of the contingency factor varied based on the type of project, the anticipated risks, and the project stage [Bradley, et al, 1990]. These single

point estimates for costs were often insufficient. Project managers realized that what was important was to model the entire range of cost variability and to understand where point estimates and cost caps fell on the distribution. In order to determine this information, cost risk analysis methods were proposed [Williams, 1995].

A cost risk model generally starts with an exhaustive decomposition of the cost items to a manageable component level, usually in a work break-down structure. Probability distributions are estimated for each cost item, and then the distributions are combined to model the probability distribution for the total cost. In some cases, a closed-form analytic solution for the convolution of the probability density functions is feasible. In practice, Monte Carlo simulation is used. In the simulation, a value for each uncertain component is drawn randomly according to its probability distribution. The entire process is then repeated for many runs. The output values then constitute a random sample from the probability distribution over the output variable induced by the input probability distributions [Burke et al., 1988, Williams, 1993, and Shishko, 1995]. This output is a cumulative distribution that estimates the expected-cost value for the project and the likelihood of exceeding certain cost levels.

Schedule risk analysis

Schedule risk involves not meeting project milestones. The primary sources of schedule risk are [Hulett, 1995]:

- lack of a realistic schedule developed to a level of detail that accurately reflects how the work will be done,
- inherent uncertainty of the work arising from advanced technology, design and manufacturing challenges, and external factors including labor relations, changing regulatory environments, and weather,
- complexity of projects that require coordination of many contractors, suppliers, government entities, etc.,
- estimates prepared in early stages of a project with inadequate definition of the work to be performed and inaccuracies or optimistic bias in estimating activity duration,
- overuse of directed (constraint) dates, perhaps in response to competitive pressures to develop aggressive, unrealistic schedules,
- project management strategies favoring late starts or fast track implementation, and
- lack of adequate float or management reserve.

The traditional schedule risk analysis model is based on the same principles as the cost analysis: an exhaustive break-down of the schedule items to a manageable component level with probability distributions estimated for each item. The major difference is that combining time in a schedule is not an additive process because of the network component. Solving a PERT network using Monte Carlo simulation means applying the longest path algorithm to a large number of realizations of task lengths, each one obtained by sampling each activity drawn from its proper distribution [Van Slyke, 1963, Moder, et al., 1983, and Williams, 1994]. The output is a cumulative distribution that estimates the expected duration of the project and the likelihood of exceeding certain schedule lengths. The simulation can also provide statistics on how frequently different paths through the network are the critical path.

Integrated methods

PERT as originally designed in the 1950s was entirely time-oriented and did not directly consider cost, availability of resources, performance, or risk. Later modifications were designed to include some of these other aspects. In 1966, GERT (Graphical Evaluation and Review Technique) was developed to allow probabilistic branching and the inclusion of costs within activities. Cost is treated as a dependent variable given certain durations for each activity. While this method includes cost and schedule uncertainties, it precludes the manager from varying the budget hypotheses and determining the potential impact on schedule [Chapman and Ward, 1997, and Lee, et al., 1982].

In 1972, the activity network model was extended to VERT (Venture Evaluation and Review Technique). VERT takes a PERT network and assigns a cost and a performance distribution to each activity. Performance can be modeled in measurable units (e.g., quantities produced) or a dimensionless index. Each arc has a set of distributions that represent the time expended, the cost incurred, and the performance generated in the completion of the specific activity that the arc represents. Rather than a joint distribution for cost, schedule, and performance, correlation coefficients are used to capture the dependencies among the three variables. The network is solved by Monte Carlo simulation where the critical path is either the path with the longest completion time, highest cost, lowest performance, or least desirable weighted combination of these factors, based on user-developed weights [Lee, et al., 1982].

Both GERT and VERT are simulation techniques and, as such, are not intended for project scheduling purposes but for analyzing potential outcomes of projects, criticality indices,

and expected values of various project parameters (time, cost, or quantities of items produced) [Weist, 1985].

Major Disadvantages of traditional project management tools for estimating risk

The cost risk analysis and schedule risk analysis tools as described are used frequently in practice [NASA JPL, 1996]. The tools are good for correcting unrealistic estimates of either cost or schedule by considering the ranges and probabilities associated with each component. Unfortunately, since the potential risks and likelihoods are aggregated by a Monte Carlo simulation, the models do not capture the relationships between the risks and potential mitigation actions. If separate cost, schedule, and technical risk analysis models are constructed, the methods do not require consistency among the models, and the effects of potential problems could be double- or triple-counted. For example, if the different risks (cost, schedule, and technical performance) are not integrated, when risk mitigation actions are taken, the project manager cannot see the impact of the solution on the other dimensions. This lack of knowledge potentially leads to sub-optimization.

While the GERT and VERT models resolve the problem of consistency among the cost and schedule risks, the inclusion of a basic performance measure (e.g., quantity of units produced) does not capture the necessary tradeoffs among cost, schedule, and technical failure risks. In addition, because the methods are based on a PERT activity network for the project, quantifying the cost, schedule, and contribution to performance for each activity in the network becomes quantitatively cumbersome and often requires somewhat unrealistic estimates of performance or quality.

2.2 Analytical Modeling Tools for Systems

Several important systems analysis tools are used to construct the overarching model in this dissertation. Descriptions follow for decision analysis and probabilistic risk analysis.

2.2.1 Decision Analysis

Decision analysis is a term used to describe “a body of knowledge for the logical illumination of decision problems” [Matheson and Howard, 1989]. The decision analysis methodology presents a systematic framework for choosing among alternative actions when the consequences of these alternatives are uncertain. An important contribution of decision analysis is a process to describe and quantify tradeoffs among alternatives. The basic steps in the decision analysis process are as follows [Covello, 1987]:

1. Define decision objectives.
2. Identify decision alternatives and all consequences that relate to the decision alternatives.
3. Define performance measures or variables for quantifying decision objectives (attributes).
4. Identify critical uncertain variables.
5. Assess probabilities for uncertain variables and scenarios.
6. Specify value judgments, preferences, and tradeoffs.
7. Evaluate alternative actions or policies.
8. Conduct sensitivity analyses and value of information analyses.

Much of the literature in this field focuses on formal methodologies that aid decision makers in balancing their preferences for possible outcomes under uncertainty. The most popular method is expected utility maximization. Most of the expected-utility decision analysis literature focuses on the formalization of the value side or preferences of the decision problem from a normative approach tailored to a single identifiable decision maker.

Expected-utility decision analysis is used in conjunction with the PPRM model to capture the decision maker's attitude toward risk and to model the decision maker's tradeoffs among the different risk elements (cost, schedule, and technical performance). The problem encountered in examining NASA's unmanned space program is uncertainty about whose values and preferences to quantify in a utility function. Potential candidates include NASA administrators, scientists, the public, or the industrial space contractors. The utility function used in the illustrations throughout this dissertation approximates the decision maker's preferences for mission outcomes by the expected costs of failure of the mission.

There are implicit assumptions in the decision analysis process that users should remember. Some of these include [Covello, 1987]:

- the decision maker is willing to reveal publicly his explicit risk preferences and value tradeoffs,
- meaningful probability and utility values can be obtained and assigned to consequences, and
- various consequences of concern to the decision maker can be made comparable to one another through utility analysis.

Additional references on decision analysis include: Keeney and Raiffa [1993], von Winterfeldt and Edwards [1986], and Keeney [1992].

2.2.2 Probabilistic Risk Analysis

Probabilistic risk analysis (PRA) provides a method to define and measure quantitatively the technical failure risks of engineering systems. The original process was developed in the commercial nuclear power industry in the 1970s [USNRC, 1975]. Since then it has been applied in many different industries including aerospace, marine off-shore oil platforms, and chemical processing. The purpose of a technical PRA is to examine all potential damage states and the frequency of each state as uncertain variables. The PRA process does not include project failures from management factors such as cancellation from budget overruns.

The general PRA process developed and used for technical systems is outlined as follows [Henley and Kumamoto, 1992, Garrick, 1984, Kaplan and Garrick, 1981, Fragola, 1994]:

Step 1: Identify the hazard(s), specifically what can happen or what can go wrong?

This includes identifying the parts of the system that give rise to the hazard(s) with event sequences that transform a hazard into an accident. Each sequence is considered a scenario, where each scenario begins with an initiating event and ends with an undesired end state. An initiating event is any abnormality, malfunction, or failure that causes a deviation from the desired operation. In between initiating events and end states are “pivotal” events that determine whether and how an initiating event propagates to an end state. Therefore, each scenario is defined by one initiating event, one or more pivotal events, and one end state.

This initial step also includes identifying all external events and their effects on the system. External events are events that originate outside the system that if they occur can impact many parts of the system at once. When examining systems for technical failures, possible external events may include earthquakes, high-winds, floods, etc.

Step 2: Determine the probability or likelihood of each scenario conditional on the occurrence or non-occurrence of external events. The fundamental difference between PRA and other risk analysis techniques (e.g., Failure Modes and Effects Analysis) is this

probabilistic step of quantifying the likelihood of the various scenarios. Quantification of the uncertainties in the context of a scenario-based risk model provides the means to identify the aspects of the problem that are the greatest risks.

Step 3: Evaluate the consequences conditional on different scenarios occurring.

Step 4: Examine the results of the analysis. The results are sets of triplets: $\langle s_i, p_i, x_i \rangle$, where s_i is a scenario identification or description; p_i is the probability of that scenario; and x_i is the consequence or evaluation measure of that scenario, (i.e., the measure of damage) [Kaplan and Garrick, 1981]. The option exists to represent the probability of the scenario as a probability distribution, for example the future frequency of an event, $p_i(\phi_i)$, rather than a discrete probability value. This alternative allows one to explicitly include the uncertainty associated with likelihood estimates. Similarly, if there is uncertainty associated with the consequences, this can also be represented as a distribution, $\zeta_i(x_i)$, [Kaplan and Garrick, 1981]. The scenarios are arranged in order of increasing severity of damage. Plotting the consequences versus the cumulative probability generates the "risk curve," or if probability distributions are used, a family of risk curves.

This dissertation includes the PRA process in a larger framework to consider simultaneously the management risks from cost and schedule overruns and the technical failure risks in projects and across programs. We quantify the probability of technical failure for a project as a function of the probability of the possible project failure modes. The PRA process is an important tool in the PPRM model to examine the tradeoffs among the different risk components and to quantify the robustness of the final project or program design.

2.3 Mars Exploration Program

The purpose of this section is to provide an overview of the Mars Program which is used for later discussions as illustrative examples of the models in this dissertation. The Mars Program is pertinent for several reasons:

- the program is still evolving and decisions concerning program architecture are still being made,
- the program has "history" on which future missions are built, and

- the program has many interesting characteristics including: mission dependencies, multiple program objectives (e.g., search for life or general space exploration), multiple missions each with its own objectives and tight constraints, many political and institutional risks (i.e., major scope changes or potential problems with foreign contributors), and high failure risks.

The US began the exploration of Mars in 1969 with the flybys of the planet by Mariners 6 and 7. Mariner 6 returned 75 photographs, and Mariner 7 returned 126 photographs. Mariner 9 orbited Mars from November 1971 until October 1972 and returned over 7,000 photographs. In 1975, the US launched two orbiter/lander spacecraft, Viking 1 in August and Viking 2 in September. The two Viking missions cost over \$3 billion (1997 dollars) and returned more than 50,000 photographs of the Mars surface. In 1992, the US launched Mars Observer, an orbiting spacecraft. Total projects costs for Mars Observer were estimated at \$500 million for spacecraft and instruments, \$100-\$150 million for operations, and \$300-350 million for launch, totaling close to \$1 billion (1997 dollars). The mission was lost on August 21, 1993, three days before it was to enter its orbit around Mars. Because of the loss of the mission, only a fraction of the operations budget was actually spent and the actual loss was in the order of \$900 million [Shirley and McCleese, 1996].

Following the failure of the Mars Observer mission in 1993, a formal, long-term program for the future exploration of Mars was established. The Mars Exploration Program is funded by NASA at approximately \$100 million per year and is expected to launch two flights to Mars during every available launch window (about every 26 months). The Mars Exploration Program includes Mars Pathfinder (with the primary payload, the Sojourner rover), Mars Global Surveyor, and the future surveyor missions (two missions in 1998, 2001, 2003, and a sample return mission in 2005). While the constraints on the future Mars missions are tight, the program aspect allows higher-level planning and optimization to meet the Mars exploration goals.

The Mars Program provides examples of projects produced under severe resource constraints that require risk tradeoffs. For example, the Mars Pathfinder lander team reduced costs with actions that could have increased the probability of technical failure. The team saved money by not building electronic spares, (e.g., only about half of the fifteen flight circuit boards had flight spares), and by not performing a high-altitude drop-test of the Viking-heritage parachute. In these cases, the additional risks were evaluated

and were considered acceptable. The rover was developed for \$25 million with very limited mass and volume. In many cases, the project team could not select the “best” parts because flight-rated components were costly or not available. The project frequently used commercial and military-specification hardware without redundancies. Therefore, a primary risk mitigation technique was component-level environmental testing (e.g., thermal, vibration, and radiation). Also, unlike a class A project where test requirements are well-specified, the system engineer and cognizant engineers had significant latitude in defining the test requirements and specifications. Consequently, the development team relied on testing to balance cost risk and technical risk.

The Mars Program also provides examples where the results of earlier projects influence the development and success of subsequent projects. Specifically, consider the Mars Global Surveyor and Deep Space 2 projects. Mars Global Surveyor (MGS) is an orbiting spacecraft designed as a rapid, low-cost recovery of the Mars Observer mission objectives. The payload for MGS includes five of the instruments originally flown on Mars Observer (reconstructed from spares) and a new communications system designed to relay scientific telemetry from future landers. One lander is the Deep Space 2 (DS2) Mars microprobe project.

The Mars 1998 lander, currently traveling to Mars (expected arrival December 1999), is carrying the DS2 microprobes to Mars. The microprobes will deploy themselves 15-20 seconds after separation of the cruise stage from the aeroshell. At impact with the surface, part of the probe will penetrate the Mars soil. The remainder of the probe will remain on the surface with the batteries and a deployable antenna for data relay through MGS. In order to save costs in designing the communications systems, the design decision was made that DS2 needs to relay data back to Earth through the MGS spacecraft, and cannot do so through the Mars 1998 orbiter [NASA JPL, 1998b].

Unfortunately, after the launch of MGS, one of the two solar arrays that power MGS did not fully deploy [NASA JPL, 1998c]. The MGS spacecraft was to alter its orbit around Mars using aerobraking, a relatively unproven technique that uses the forces of atmospheric drag to slow the spacecraft into its final orbit. With the damaged solar array, the aerobraking maneuvers were much more risky. If the MGS spacecraft had been lost in attempting to reach the correct orbit with aerobraking, then the DS2 project would also be lost. Fortunately, MGS was able to lengthen their aerobraking schedule and reach an

acceptable orbit in February 1999. This situation represents the types of problems and dependencies that exist in programs of projects.

Studying the Mars Program proved useful in formulating the PPRM model. The projects were conducted with little redundancy and demonstrated the potential interdependencies among projects. The projects were produced under tight resource constraints that required risk tradeoffs throughout development. Several of the key decisions highlighted by both the empirical studies reviewed above and by the Mars Program include:

- how to manage projects that are parts of larger programs,
- how to set project specifications, including what fraction of a project budget to hold as reserves,
- how to manage the resources to minimize the probability of technical failure,
- how to allocate management reserves to potential problems during project development to minimize the probability of management failure,
- when to relax constraints or reduce project scope,
- when to develop new technology, and
- how to establish an effective problem detection and warning system to detect potential defects.

These issues are illustrated in the presentation of the PPRM model in the remainder of this dissertation.

CHAPTER 3

Probabilistic Program Risk Management (PPRM) Model Case 1- One Project

3.1 Introduction to the PPRM Model

Most analysis performed to support decision making in project management focuses on either technical risks or management risks. The PPRM model quantifies both these risks and the tradeoffs between them. The model is structured into three sequential optimization steps. Figure 3.1 shows the relationship of the model steps to the risk components for a project.

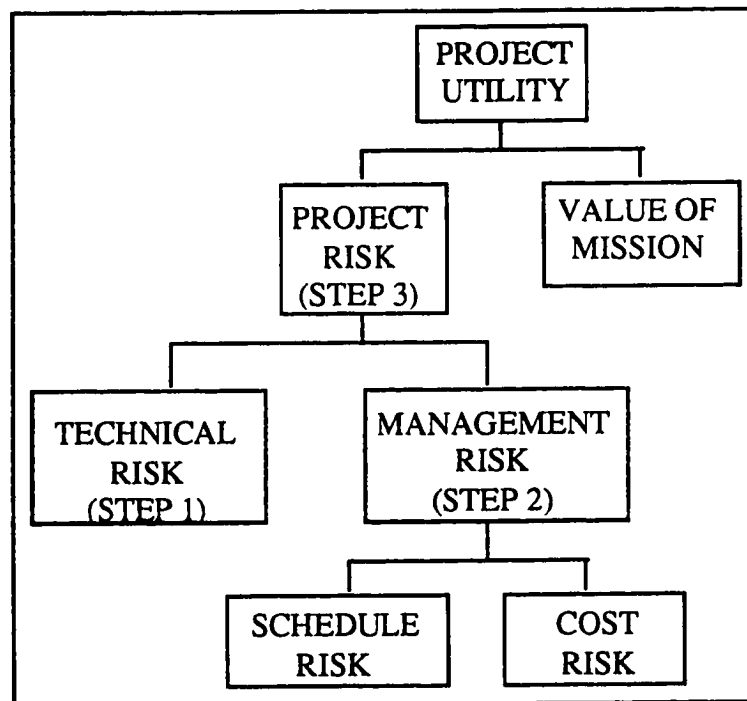


Figure 3.1- Risk Components and PPRM Steps

The steps are:

STEP 1: Develop and optimize all feasible technical design alternatives (configuration and choice of components) over the range of potential project development budgets to minimize each alternative's probability of technical failure.

STEP 2: For each technical design alternative, optimize the strategy to reduce management risks over the range of potential reserve budgets, where the strategy is determined by:

- the potential management problems that could occur for each technical design alternative, and
- potential mitigation actions for each management problem.

STEP 3: Determine the optimal technical design alternative and the budget reserve based on the lowest overall expected failure cost given the optimal management risk strategies for that design.

The implementation of this optimization algorithm is examined for a series of cases. The remainder of this chapter describes Case 1. In Case 1, a fixed project budget is optimally allocated between the project development budget and the reserves with a fixed portion of the development budget required for risk analysis. These allocation decisions directly affect the probabilities of different types of failure for the mission. For example, allocating more money to the development budget (and less to reserves) may increase the technical reliability of the mission. Failure to maintain sufficient reserves, however, could critically affect the project should development problems occur. This allocation decision is represented in Figure 3.2 by the adjustable division between the design and development budget and the project reserves.

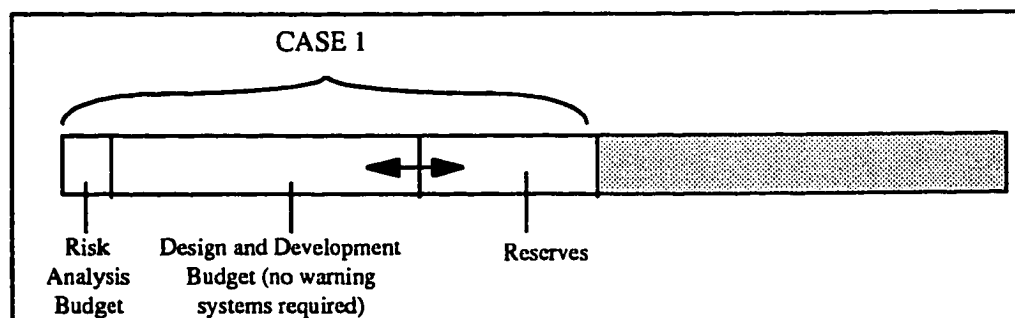


Figure 3.2- Case 1: Budget Allocation Between Development and Reserves

Case 1 assumes that as soon as problems occur during development, they are detected, and thus the resources required for "warning systems" (i.e., reviews and testing) are implicitly included in the development budget. In Case 2, described in Chapter 4, we relax this assumption and use the PPRM model to evaluate the choice of a warning system for the project. Case 1 also assumes that all technical and management failures result in the total

loss of the mission. We do not consider here the possibility of partial failures. The removal of this assumption is considered in Case 3, described in Chapter 5. Finally, Case 1 assumes that each project is developed and operated independently from the rest of the program, (i.e., no other projects depend on the outcome of this project). We remove this assumption in Case 4, described in Chapter 6, when we examine programs of interdependent projects.

The outputs of the PPRM model for Case 1 are (1) the recommended functional design configuration and components for the project, and (2) the development budget and corresponding reserve budget. Section 3.2 describes the details of each of the three steps in the PPRM model applied to Case 1, and Section 3.3 provides an illustration of the model.

3.2 PPRM Model Description for Case 1

The following notation is used in describing the PPRM model:

Management failure of project (Boolean): MF

Technical failure of project (Boolean) (technical failure by definition assumes no MF): TF

Possible failure states (indexed in i) for project: $FS_i \in \{MF, TF\}$

Cost impact of outcome state FS_i : $C(FS_i)$

Project success (no failure occurs): \overline{FS}

Project technical failure modes (each is associated to the failure of one of the critical subsystems, subsystems indexed in s): FM_s

Total budget for project (assume fixed): C

Development budget: DC

Reserve budget: RC

Risk analysis budget: RA

Total schedule duration for project (assume fixed): S

Development duration: DS

Schedule reserves: RS

Development problem that occurs on project (assume problem independence), indexed in n: DP_n

Development problem scenarios, ranked by probable chronology of problems, where each problem can either occur or not occur (Boolean sequence), indexed in ℓ : DPS_ℓ

Set of indices of all problems that occur during the development phase: $\{n_\ell\}$

Optimal risk management actions given development problem scenario DPS_ℓ : RM_ℓ^*

Cost of optimal risk management strategy RM_ℓ^* : $C(RM_\ell^*)$

Schedule duration of optimal risk management strategy RM_ℓ^* : $S(RM_\ell^*)$

Set of functional configurations for the project: $FIG = \{FIG_1, \dots, FIG_z, \dots\}$

Set of feasible technical design alternatives (z is the index of possible configurations, w is the index of one alternative choice of components for a configuration): $AFIG = \{AFIG_{1,1}, \dots, AFIG_{z,w}, \dots\}$

The following is a detailed description for implementing the PPRM model.

STEP 1: Optimize technical design alternatives.

Step 1.1 Identify the technical functions of the project given the mission scope.

Step 1.2 Identify the set of functional configurations available for implementing the project. Define this set $FIG = \{FIG_1, \dots, FIG_z, \dots\}$. Figure 3.3 is an example of one possible functional configuration for an unmanned space mission with redundancy in the communications and power subsystems. A different functional configuration is a completely single-string design.

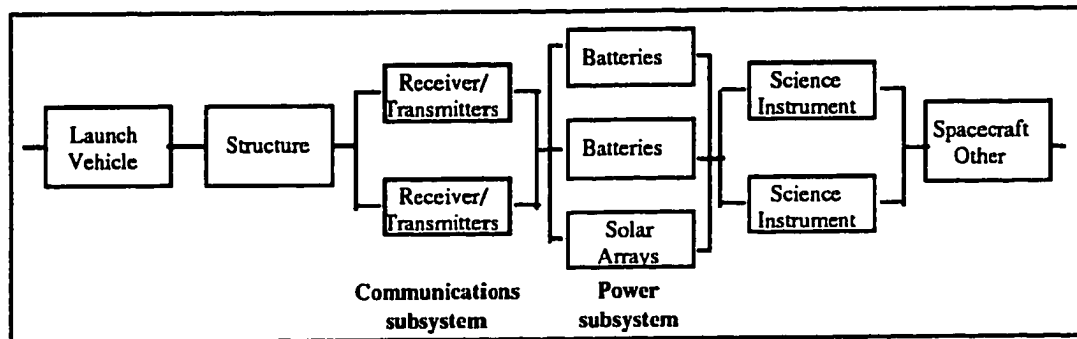


Figure 3.3- One Possible Functional Configuration (FIG_z)

Step 1.3 For each functional configuration, many different components or parts could be selected (e.g., lithium batteries or nickel cadmium). Define AFIG as the set of functional configurations and associated components. $AFIG = \{AFIG_{1,1} \dots AFIG_{z,w}, \dots\}$

Step 1.4 For each functional configuration, determine $AFIG_{z,min}$, the lowest-cost alternative. Figure 3.4 shows the relationship of the cost of $AFIG_{z,min}$ to the total available project budget (C).

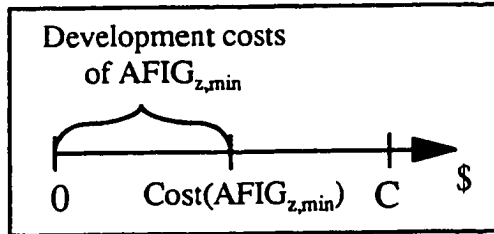


Figure 3.4- Lowest-Cost Alternative for Configuration z ($AFIG_{z,min}$)

Step 1.5 Fix the risk analysis budget and schedule allocation. The risk analysis budget includes all resources allocated to studying the potential problems, risks, mitigation actions, and probabilities of failure for the project. Currently, the schedule reserve is a factor in the probability of management failure, and we do not consider reallocating schedule between development and reserves. The capability to vary this parameter will be explored in future work.

Step 1.6 Determine the feasible subset of $\{AFIG_{z,min}\}$ based on total budget, schedule, mass, volume, etc.

Step 1.7 For each feasible functional configuration, vary the amount allocated to development and compute the resulting budget surplus as follows:

$$\text{Budget surplus} = \text{Portion of Budget Allocated to Design} - \text{Cost of Risk Analysis} - \text{Cost}(AFIG_{z,min}) \quad (3.1)$$

For example, if the cheapest design for the configuration is \$100 million, allocating 100% of a \$150 million budget to design generates a budget surplus of \$50 million less the cost of the risk analysis.

Step 1.8 Use a PRA model of the configuration and the Karush-Kuhn-Tucker optimization algorithm to optimize the design based on the cost of improvements, the budget surplus, and associated contributions to the reduction of technical risk : $p(\text{TF}|\text{AFIG}_{z,\text{min}})$.

The Karush-Kuhn-Tucker [Hillier and Lieberman, 1990] optimization algorithm is a method for optimizing constrained nonlinear programming problems using Lagrange multipliers. The objective is to minimize the probability of technical failure given the technical design alternative as a function of the failure modes of the system:

$$\text{Minimize: } p(\text{TF}|\text{AFIG}_{z,w}) = \sum_i p(\text{FM}_i|\text{AFIG}_{z,w}) - \text{"doubles"} + \dots \quad (3.2)$$

The probability of the failure mode is defined by the functional configuration of the subsystem (i.e., single string, redundant components within the subsystem, etc.) and the investment allocated to reinforce the subsystem (and therefore the w , where w is an alternative choice of components). The minimization problem is constrained so that the investments in reinforcing the subsystems is less than or equal to the budget surplus.

RESULTS OF STEP 1: After completing step 1, the project manager has identified a set of functional configurations and for each of them, the optimal choice of components given all potential levels of budget surplus.

STEP 2: Optimize the strategy to reduce management risks.

Step 2.1 For each technical design alternative, construct development problem scenarios and possible risk mitigation responses to determine the optimal risk management strategy RM_ℓ^* for each scenario ℓ . These development problem scenarios and mitigation responses are structured in a decision tree similar to the example in Figure 3.5. Rectangular nodes represent decision points and circular nodes represent chance nodes. In evaluating a decision tree, the principle is to start from the end branches and "roll back" to the base, at each chance node calculating the expected utility, and at each decision node choosing the branch with the maximum expected utility. This process generates the best sequence of decisions to maximize the expected utility of the decision maker.

This process requires a detailed list of the possible problems that can occur. For the truly unexpected problems, an additional "unanticipated problem node" can be included to account for the unknowns with either the mitigation costs of the average of the identified problems or some other reasonable estimate.

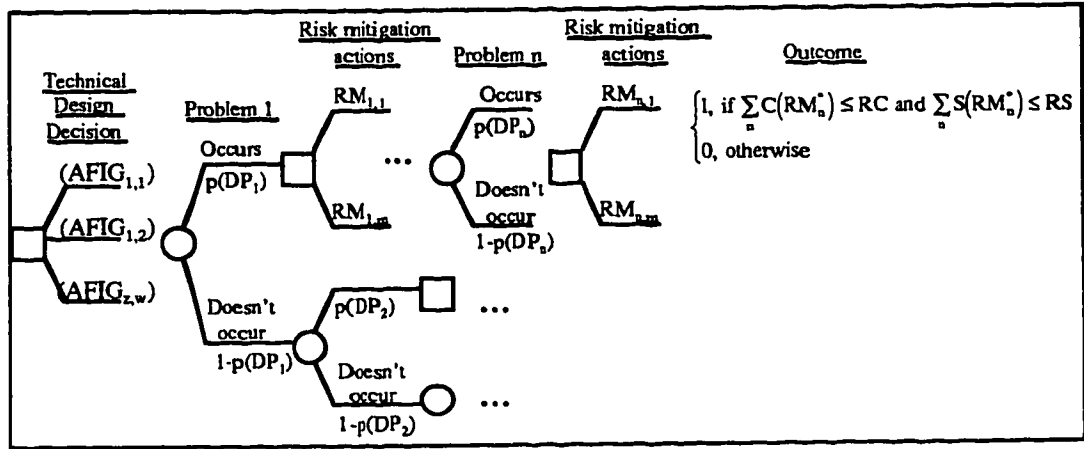


Figure 3.5- Example Decision Tree

Step 2.2 Resolve the decision tree to determine the probability of each scenario ℓ . The probability of design problem scenario ℓ is the product of the probabilities of development problems that occur multiplied by the product of the complements of the probabilities of development problems that do not occur:

$$p(\text{DPS}_\ell) = \prod_{r \in \{n_\ell\}} p(\text{DP}_r) \times \prod_{r \in \{n_\ell\}} [1 - p(\text{DP}_r)] \quad (3.3)$$

Step 2.3 Determine the outcome for each scenario, conditional on the optimal sequence of risk management options. Define an indicator variable, γ , where $\gamma = 1$ if the optimal risk mitigation strategy for scenario ℓ , RM_ℓ^* , does not exceed cost or schedule reserves given the development problem scenario, DPS_ℓ , and $\gamma = 0$ otherwise:

$$\gamma = \begin{cases} 1, & \text{if } C(\text{RM}_\ell^*)|\text{DPS}_\ell \leq RC \text{ and } S(\text{RM}_\ell^*)|\text{DPS}_\ell \leq RS \\ 0, & \text{otherwise management failure} \end{cases} \quad (3.4)$$

Step 2.4 For each design alternative, determine the probability of management failure given the corresponding reserves and the optimal mitigation strategy determined above. The probability of management failure conditional on the technical design alternative is one minus the sum of the outcome of each design problem scenario as defined by the indicator variable γ multiplied by the probability of that scenario:

$$p(\text{MF}|\text{AFIG}_{z,w}) = 1 - \sum_\ell (\gamma|\text{AFIG}_{z,w}, \text{DPS}_\ell) \times p(\text{DPS}_\ell). \quad (3.5)$$

If more resources are allocated to the project reserves, the project team can solve more potential problems, and thus reduce the probability of management failure. The trade-off between schedule and budget is accounted for on a case-by-case basis in the identification of RM_i^* in scenario ℓ to minimize the probability of management failure.

RESULTS OF STEP 2: After completing step 2, the project manager has for each of the technical design alternatives developed in step 1, an optimal risk mitigation strategy for all conjunctions of identifiable development problems as a function of the reserves available.

STEP 3: Determine the optimal technical design alternative based on the lowest overall expected failure cost.

Step 3.1 For each alternative, $AFIG_{z,w}$, and the corresponding remaining budget reserve (assuming schedule reserve is fixed), compute the overall expected failure cost. The expected failure cost is the sum of the cost of each failure state multiplied by the probability of that state, assuming that a successful project outcome state has zero failure costs:

$$E(AFIG_{z,w}) = C(MF) \times p(MF|AFIG_{z,w}) + C(TF) \times p(TF|AFIG_{z,w}). \quad (3.6)$$

Step 3.2 Determine the optimal design alternative. First, find the optimal components for each configuration, then determine the overall optimal among all configurations. The development cost of the optimal design alternative determines the level of budget reserves that minimizes the expected failure cost.

Figure 3.6 summarizes the optimization algorithm.

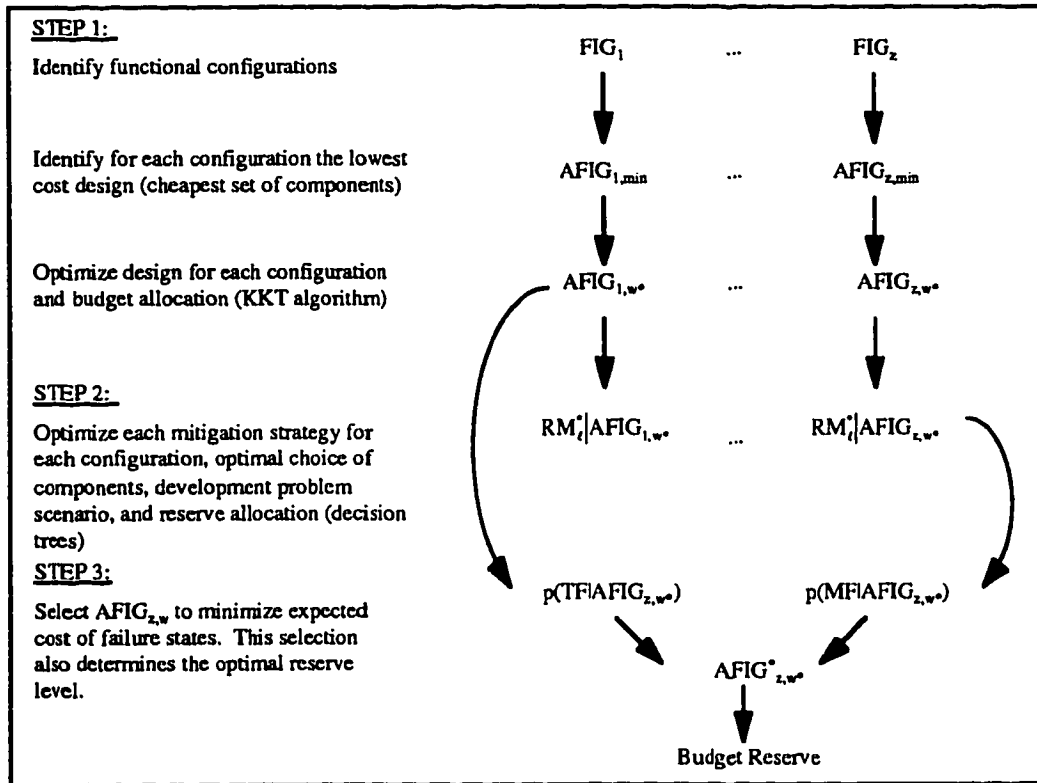


Figure 3.6- Summary of Optimization Algorithm

3.3 Illustration of the Model for Case 1

Assume that a project manager is developing a planetary orbiter mission with a budget of \$150 million (including the launch vehicle) and a schedule duration of 3 years. The spacecraft has two instruments: a gamma ray spectrometer and a camera. He or she is using the PPRM model, to determine the optimal technical design alternative and the amount of budget to be retained for reserves.

STEP 1: Optimize technical design alternatives.

Step 1.1 Identify the spacecraft functions given the scope of the mission.

The spacecraft functional block diagram is shown in Figure 3.7.

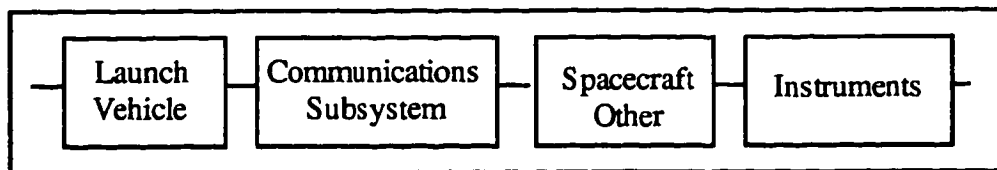


Figure 3.7- Case 1: Spacecraft Functional Block Diagram

Step 1.2 Identify the set of functional configurations. Define this set $FIG = \{FIG_1, \dots, FIG_z, \dots\}$.

Two functional configurations are being considered here. Figure 3.8 shows configuration 1, a single-string design, and Figure 3.9 shows configuration 2, a partially redundant system (two receiver/transmitters in parallel).

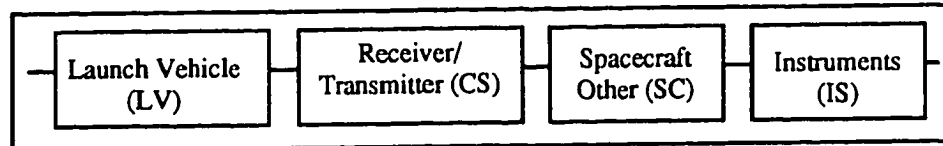


Figure 3.8- Case 1: Single-string design, $z = 1$

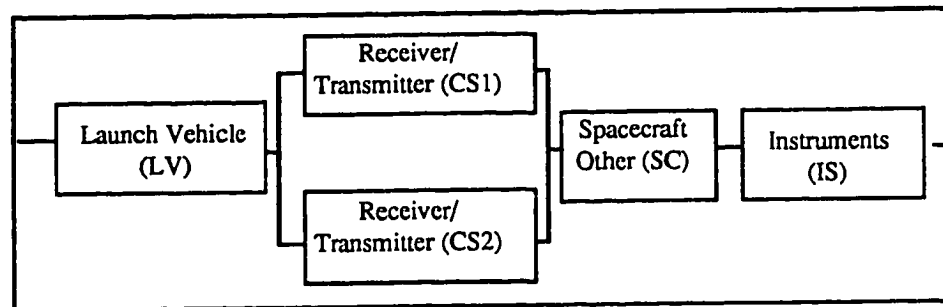


Figure 3.9- Case 1: Spacecraft with Redundant Communications System, $z = 2$

Step 1.3 Define AFIG as the set of functional configurations and associated components.

$$AFIG = \{AFIG_{1,1} \dots AFIG_{z,w}, \dots\}$$

Step 1.4 For each functional configuration, determine $AFIG_{z,min}$ the lowest-cost alternative.

$$\text{Assume } \text{Cost}(AFIG_{1,min}) = \$124 \text{ million, } \text{Cost}(AFIG_{2,min}) = \$129 \text{ million}$$

Step 1.5 Fix the risk analysis budget and the schedule allocation.

Risk analysis budget is \$1 million. Development schedule has been set at 34 months with 2 months of schedule reserves.

Step 1.6 Determine the feasible subset of $\{AFIG_{z,min}\}$.

Both configuration 1 and configuration 2 are feasible in terms of budget and schedule.

Step 1.7 For each feasible functional configuration, vary the amount allocated to development and compute the resulting budget surplus as follows:

$$\text{Budget surplus} = \text{Portion of Budget Allocated to Design} - \text{Cost of Risk Analysis} - \text{Cost}(AFIG_{z,min}) \quad (3.8)$$

\$0 < Budget surplus for configuration 1 < \$25 million
 \$0 < Budget surplus for configuration 2 < \$20 million

Step 1.8 Use a PRA model of the configuration and the Karush-Kuhn-Tucker algorithm to optimize the design based on the cost of improvements, the budget surplus, and associated contributions to the reduction of technical risk : $p(TF|AFIG_{z,w})$.

We first optimize the design alternatives for configuration 1, the single-string design. We then repeat the optimization process for configuration 2, the partially redundant system.

Configuration 1 (single-string)

Table 3.1 shows the probabilities of the failure modes for the subsystems in $AFIG_{1,min}$, assuming that all basic event failures are independent.

Table 3.1- Case 1: Probability of Failure Modes, Configuration 1

Subsystem	$p(FM_s AFIG_{1,min})$
Launch Vehicle	0.1
Communications Subsystem	0.1
Spacecraft	0.01
Instruments Package	0.05

The probability of technical failure for the lowest-cost design for configuration 1 is:

$$\begin{aligned} p(TF|AFIG_{1,min}) &= \sum_{s \in \{LV,CS,SC,IS\}} p(FM_s|AFIG_{1,min}) - \text{"doubles"} + \dots \\ &= 0.23 \end{aligned} \quad (3.9)$$

We then consider possible reductions of the probability of technical failure given investments in improvements above the minimum or cheapest components. We assume in all of the illustrations in this dissertation that the probability of failure decreases continuously (here exponentially) with financial investments in reinforcement, i.e.,

$p(FM_s|AFIG_{z,w}) = p(FM_s|AFIG_{z,min}) \times \text{Exp}[-K_s I_s]$, where I_s is the investment to reinforce subsystem s and K_s is an assessed constant.

Assume that the spacecraft manager cannot improve the reliability of the launch vehicle. Also assume that the effects of investment in reinforcing the spacecraft are as described in Table 3.2.

Table 3.2- Case 1: Effects of Investment on Reinforcement of Configuration 1

Subsystem	Investment	Reduction Factor	$p(FM_s AFIG_{i,w})$
Launch Vehicle	n.a.	n.a.	0.1
Communications Subsystem	\$12 M	10	$0.1 \times \text{Exp}[-0.192 I_{CS}]$
Spacecraft	\$10 M	10	$0.01 \times \text{Exp}[-0.23 I_{SC}]$
Instruments Package	\$10 M	10	$0.05 \times \text{Exp}[-0.23 I_{IS}]$

Using the relationships between investment and increased robustness, the optimal design alternative is determined by minimizing the probability of technical failure subject to the constraint that the total amount invested reinforcing the system is equal to the budget surplus available for reinforcement:

$$\begin{aligned}
 p(TF|AFIG_{i,w}) = & 0.1 + 0.1 \times \text{Exp}[-0.192 I_{CS}] + 0.01 \times \text{Exp}[-0.23 I_{SC}] + \\
 & 0.05 \times \text{Exp}[-0.23 I_{IS}] - 0.01 \times \text{Exp}[-0.192 I_{CS}] - \\
 & 0.001 \times \text{Exp}[-0.23 I_{SC}] - 0.005 \times \text{Exp}[-0.23 I_{IS}] - \\
 & 0.001 \times \text{Exp}[-0.192 I_{CS} - 0.23 I_{SC}] - 0.005 \times \text{Exp}[-0.192 I_{CS} - 0.23 I_{IS}] - \\
 & 0.0005 \times \text{Exp}[-0.23 (I_{CS} + I_{IS})]
 \end{aligned} \tag{3.10}$$

so that $I_{CS} + I_{SC} + I_{IS} = \text{Budget surplus available for reinforcement}$.

Figure 3.10 shows on one y-axis, the optimal investment in each subsystem for various levels of investment, and on the second y-axis, the effect of various levels of investment on the probability of technical failure for the system. For example, if \$9 million is invested in reinforcing the system, then at the optimum, \$6.1 million is invested in the communications subsystem, \$2.9 million is invested in the instrument package, and the resulting probability of technical failure for the reinforced system is 0.16.

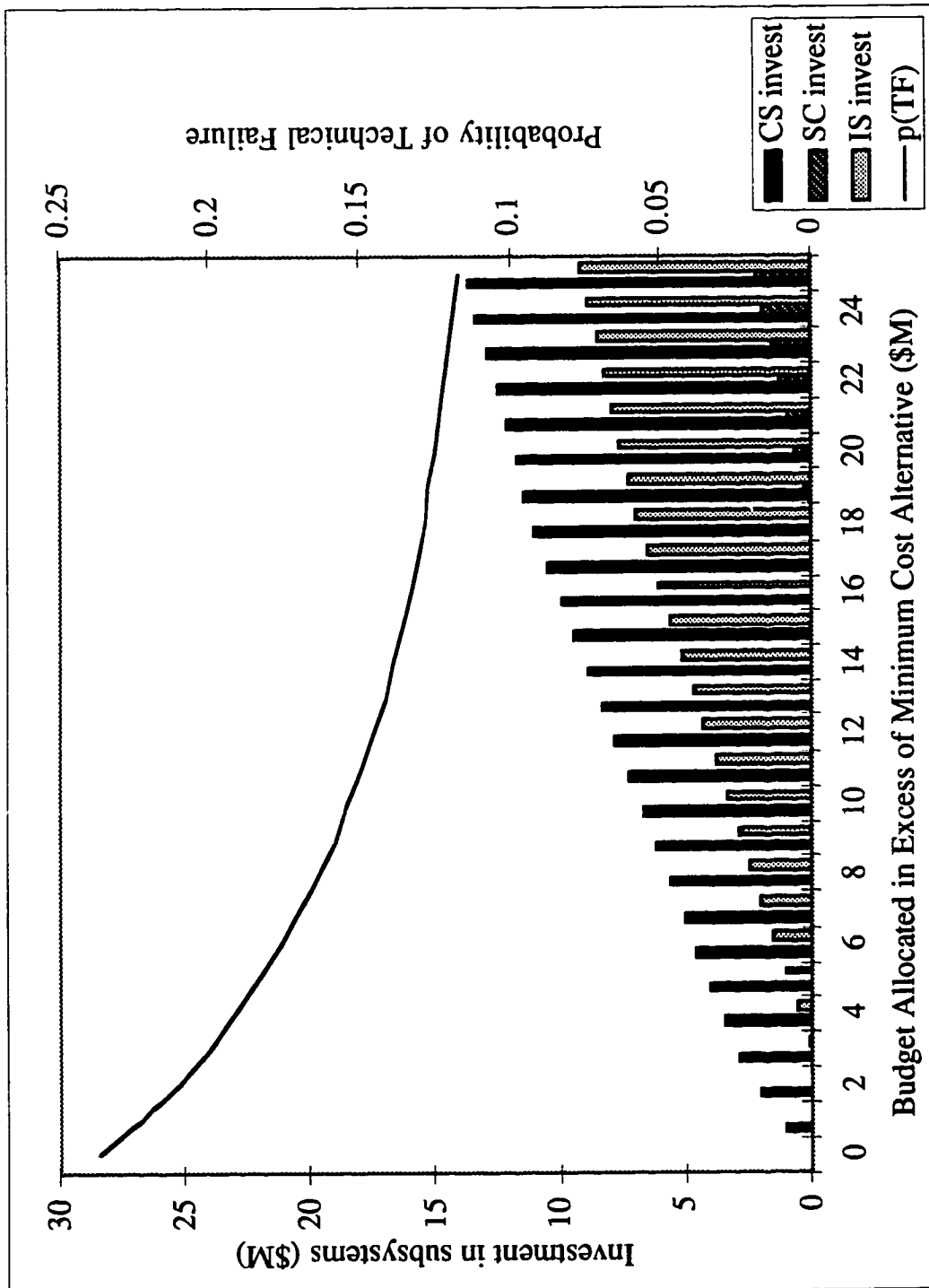


Figure 3.10- Case 1: Various Investment Levels for Configuration 1

Configuration 2 (with redundant communications subsystem)

Table 3.3 shows the probabilities of the failure modes for the subsystems in $AFIG_{2,min}$, assuming that all basic event failures are independent.

Table 3.3- Case 1: Probability of Failure Modes, Configuration 2

Subsystem/ Component	Subsystem Failure $p(FM_s AFIG_{2,min})$
Launch Vehicle	0.1
Communications Subsystem	$p(F_{CS1} AFIG_{2,min}) \times$ $p(F_{CS2} F_{CS1}, AFIG_{2,min}) =$ $0.1 \times 0.1 = 0.01$
Spacecraft	0.01
Instruments Package	0.05

The probability of technical failure for the lowest-cost design for configuration 2 is:

$$p(TF|AFIG_{2,min}) = \sum_{s \in \{LV,CS,SC,IS\}} p(FM_s|AFIG_{2,min}) - \text{"doubles"} + \dots \quad (3.11)$$

$$= 0.16$$

Repeating the optimization process for configuration 2, we consider possible reductions of the probability of technical failure given investments in improvements above the minimum or cheapest components, using the data provided in Table 3.4. Figure 3.11 shows on one y-axis, the optimal investment in each subsystem for various levels of investment, and on the second y-axis, the effect of various levels of investment on the probability of technical failure for the system for configuration 2.

Table 3.4- Case 1: Effects of Investment on Reinforcement of Configuration 2

Subsystem/ Component	Investment	Reduction Factor
Launch Vehicle	n.a.	n.a.
Communications Component 1	\$12M	10
Communications Component 2	\$12M	10
Spacecraft	\$10M	10
Instruments Package	\$10M	10

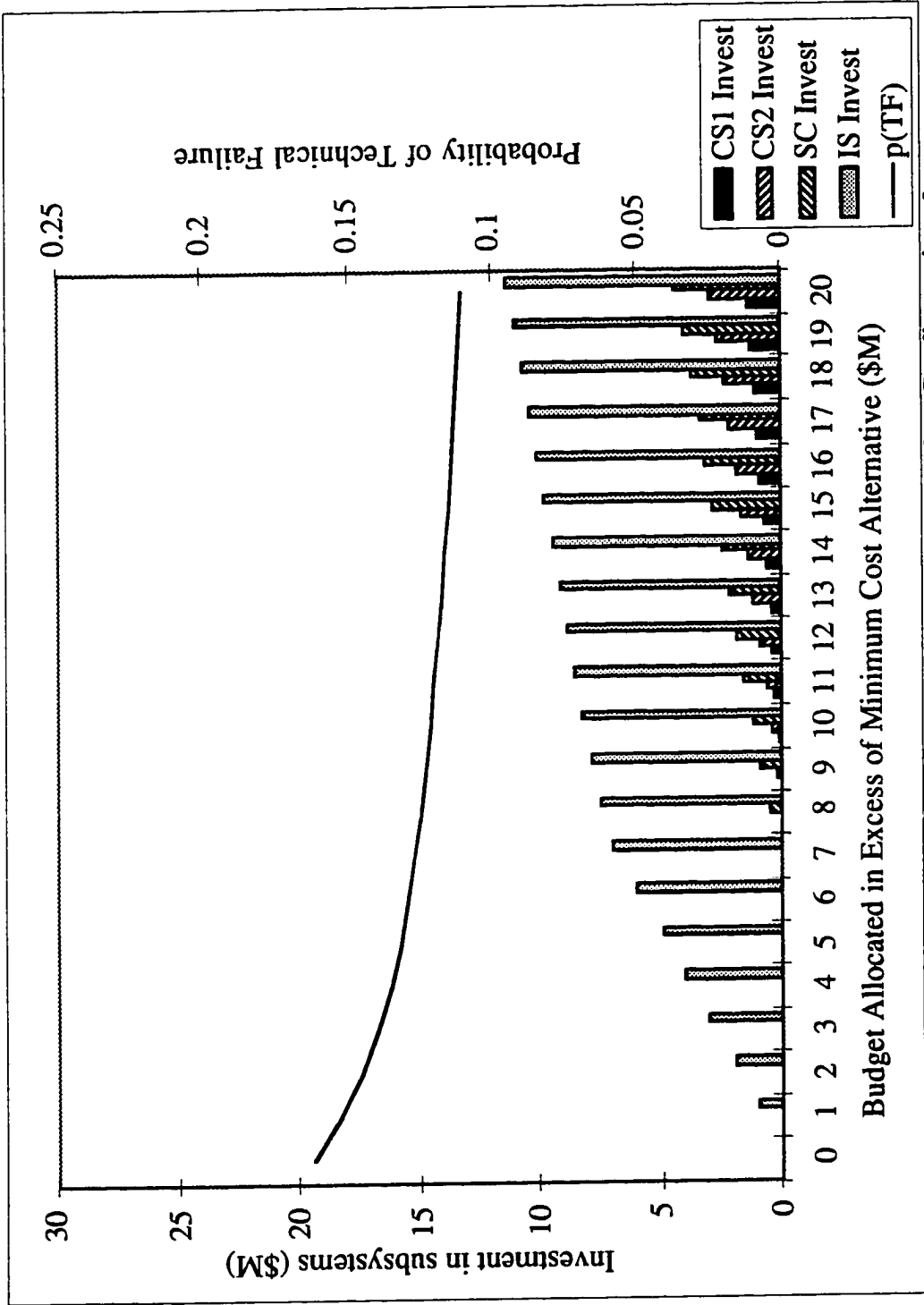


Figure 3.11- Case 1: Various Investment Levels for Configuration 2

Results of Step 1

After completing Step 1, the project manager has identified a set of two functional configurations, one single-string and one partially redundant, and for each of them the optimal set of components as shown in Figures 3.10 and 3.11 for all potential levels of development budget.

STEP 2: Optimize the strategy to reduce management risks.

Step 2.1 For each technical design alternative, construct development problem scenarios and possible risk mitigation responses.

Table 3.5 shows the potential problems and risk mitigation alternatives for configuration 1. Table 3.6 shows the corresponding data for configuration 2. For each potential problem, the project manager has at least two mitigation strategies: (1) an action where the problem is resolved entirely with budget reserves and has no impact on schedule reserves or technical performance, or (2) an action where the problem is resolved for less cost but requires some schedule slippage. Several of the problems also have a third mitigation alternative that has no cost or schedule implications, and instead has performance impacts. This third mitigation alternative is considered in Case 3 when partial project failures are possible. Because of the redundant communications subsystem in configuration 2, both the probability of a potential integration problem and the mitigation costs are greater than for configuration 1. The differences are shaded in Table 3.6.

Table 3.5- Case 1: Management Risk Data for Configuration 1

Potential Problems (Risks) conditional on technical design	Probability	Mitigation Alternative 1 (Solve with \$)	Mitigation Alternative 2		Other Mitigation Alternatives
			(Cost)	(Sch.)	
modem procurement prob.	0.4	\$5 M	\$3 M	1 mo.	n.a.
software development prob.	0.2	\$5 M	\$3 M	1 mo.	simplify software
communications integration problem	0.3	\$3 M	\$2 M	0.5 mo.	n.a.
insufficient test personnel	0.5	\$3 M	\$1.5 M	1 mo.	reduce testing
late instrument delivery	0.2	\$3 M	\$1.5 M	1 mo.	substitute instrument
instrument power problems	0.1	\$3 M	\$1.5 M	1 mo.	n.a.
spacecraft mass problems	0.1	\$3 M	\$2 M	1 mo.	n.a.
Unknown problems	0.5	\$5 M	\$3 M	1 mo.	n.a.

Table 3.6- Case 1: Management Risk Data for Configuration 2

Potential Problems (Risks) conditional on technical design	Probability	Mitigation Alternative 1 (Solve with \$)	Mitigation Alternative 2		Other Mitigation Alternatives
			(Cost)	(Sch.)	
modem procurement prob.	0.4	\$5 M	\$3 M	1 mo.	n.a.
software development prob.	0.2	\$5 M	\$3 M	1 mo.	simplify software
communications integration pb.	0.6	\$5 M	\$3 M	0.5 mo.	n.a.
insufficient test personnel	0.5	\$3 M	\$1.5 M	1 mo.	reduce testing
late instrument delivery	0.2	\$3 M	\$1.5 M	1 mo.	substitute instrument
instrument power problems	0.1	\$3 M	\$1.5 M	1 mo.	n.a.
spacecraft mass problems	0.1	\$3 M	\$2 M	1 mo.	n.a.
Unknown problems	0.5	\$5 M	\$3 M	1 mo.	n.a.

Figure 3.12 shows a portion of the decision tree constructed from these problems and potential mitigation actions. The preferred sequence of mitigation actions is identified by arrows in the diagram. A 0 at the end of the branch denotes a management failure from either a cost or a schedule overrun, and a 1 at the end of the branch represents a successful mitigation strategy (i.e., does not exceed the reserves).

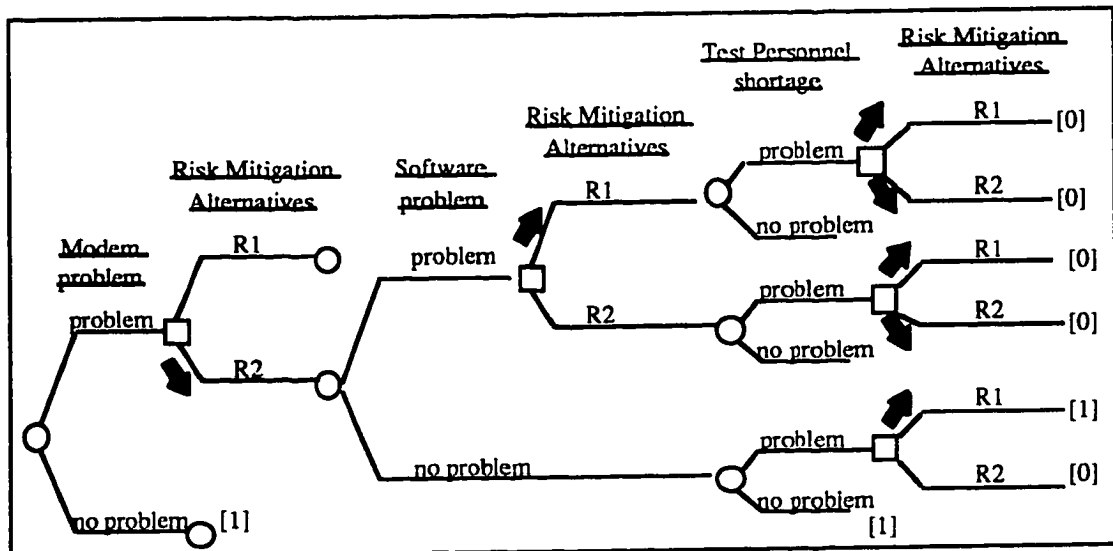


Figure 3.12- Case 1: Portion of the Decision Tree for Configuration 1

Step 2.2 Resolve the decision tree to determine the probability of each scenario l .

Completed by decision tree resolution (using Precision Tree software) [Palisade Corporation, 1997].

Step 2.3 Determine the outcome for each scenario, conditional on the optimal sequence of risk management options.

Completed by decision tree resolution (using Precision Tree software) [Palisade Corporation, 1997].

Step 2.4 For each design alternative, determine the probability of management failure given the corresponding reserves and the optimal mitigation strategy determined above.

$$p(\text{MF}|\text{AFIG}_{z,w}) = 1 - \sum_l (\gamma_l | \text{AFIG}_{z,w}, \text{DPS}_l) \times p(\text{DPS}_l) \quad (3.12)$$

Figure 3.13 shows the results for both configuration 1 and configuration 2 of the probability of management failure as a function of the reserve allocation.

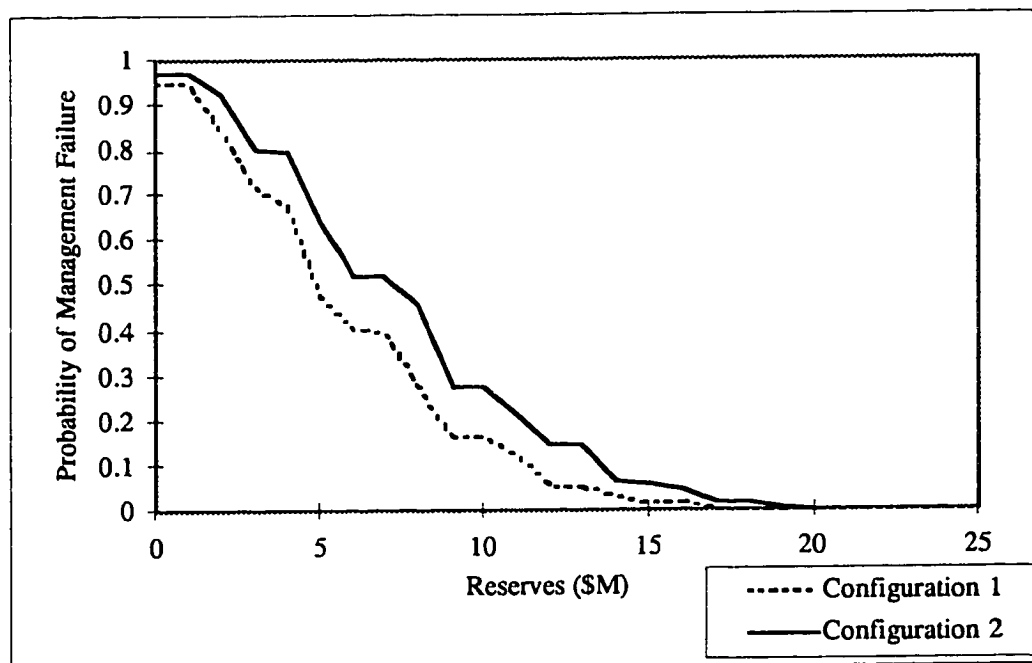


Figure 3.13- Case 1: Probability of Management Failure as a Function of the Reserve Allocation for Configurations 1 and 2

Results of Step 2

After completing step 2, the project manager has, for each of the technical design alternatives, a decision tree that shows the optimal risk mitigation strategy as a function of the optimal choice of components and the corresponding available reserve.

STEP 3: Determine the optimal technical design alternative based on the lowest overall expected failure cost.

Step 3.1 For each alternative, $AFIG_{z,w}$, and the corresponding remaining budget reserve, compute the overall expected failure cost:

$$E(AFIG_{z,w}) = C(MF) \times p(MF|AFIG_{z,w}) + C(TF) \times p(TF|AFIG_{z,w}). \quad (3.13)$$

Assume that the Cost(TF) is \$150 M, and that the Cost(MF) is \$150 M. Table 3.7 shows the results of optimal design choices for configuration 1. The best technical design alternative for configuration 1 (i.e., the lowest achievable expected cost of failure) is obtained by spending \$135 million on development and keeping \$15 million in reserves. Table 3.8 shows the results of optimal design choices for configuration 2. The best technical design alternative for configuration 2 is obtained by spending \$133 million on development and keeping \$17 million in reserves. The development costs in both tables include \$1 million for the project risk analysis.

Table 3.7- Case 1: Design Alternatives for Configuration 1
(Total Available Budget = \$150M)

Development (M)	p(TF)	Reserves (M)	p(MF)	E(Cost of Failure (\$M))
\$150	0.12	\$0	0.95	143.4
\$145	0.13	\$5	0.48	82.1
\$140	0.14	\$10	0.16	41.6
\$139	0.14	\$11	0.12	36.5
\$138	0.14	\$12	0.05	27.5
\$137	0.15	\$13	0.05	28.9
\$136	0.15	\$14	0.03	26.3
\$135	0.15	\$15	0.02	25.1
\$134	0.16	\$16	0.02	26.5
\$133	0.16	\$17	0.01	25.3
\$132	0.17	\$18	0.00	25.5
\$131	0.18	\$19	0.00	27.0
\$130	0.18	\$20	0.00	27.0
\$125	0.24	\$25	0.00	36.0

Table 3.8- Case 1: Design Alternatives for Configuration 2
(Total Available Budget = \$150M)

Development (M)	p(TF)	Reserves (M)	p(MF)	E(COST OF FAILURE) (\$M)
\$150	0.11	\$0	0.97	146.0
\$149	0.11	\$1	0.97	146.0
\$148	0.11	\$2	0.92	139.3
\$147	0.11	\$3	0.80	123.3
\$146	0.11	\$4	0.80	123.3
\$145	0.12	\$5	0.64	102.5
\$140	0.12	\$10	0.28	55.0
\$139	0.12	\$11	0.22	47.0
\$138	0.13	\$12	0.15	39.1
\$137	0.13	\$13	0.15	39.1
\$136	0.13	\$14	0.07	28.6
\$135	0.13	\$15	0.06	27.3
\$134	0.14	\$16	0.05	27.5
\$133	0.14	\$17	0.02	23.6
\$132	0.15	\$18	0.02	25.1
\$131	0.15	\$19	0.01	23.8
\$130	0.16	\$20	0.00	24.0

Step 3.2 Determine the optimal design alternative.

The recommended alternative for this illustration (corresponding to the minimum expected cost of failure) is to:

- Choose configuration 2 (the partially redundant system)
- Keep \$17 million in reserves
- Spend \$133 million in development (including \$1 million for risk analysis and \$3 million for the reinforcement of the instrument package (as shown in Figure 3.11))

In this illustration, the redundant system is preferred to the single-string system because the selection of a redundant configuration results in the lowest achievable expected cost of failure. The probability of technical failure is lower and more resources are allocated to the reserves.

Shadow Cost of Budget Constraint

Table 3.9 examines the sensitivity of this recommendation with slight changes in the budget constraint. If more money is allocated to the mission, configuration 2 is still optimal and the additional budget is spent initially to reinforce the system and then to reduce the probability of management failure. If the budget is reduced by more than \$3 million, the

simpler, single-string configuration is preferred, primarily because the simpler system has a lower probability of management failure for the same amount of reserves.

Table 3.9- Case 1: Shadow Cost of Budget Constraint

± Constraint (orig. \$150M)	Config	Develop. (M)	p(TF)	Reserves (M)	p(MF)	E(Cost of Failure) (M)	ΔE (M)
+\$1 M	1	\$136	0.15	\$15	0.016	\$24.4	-0.6
	2	\$134	0.14	\$17	0.021	\$23.0	
+\$2 M	1	\$135	0.15	\$17	0.005	\$23.7	-1.5
	2	\$133	0.14	\$19	0.009	\$22.1	
+\$3 M	1	\$136	0.15	\$17	0.005	\$23.0	-2.2
	2	\$134	0.14	\$19	0.009	\$21.4	
+\$4 M	1	\$139	0.14	\$15	0.016	\$22.9	-2.7
	2	\$134	0.14	\$20	0.005	\$20.9	
+\$5 M	1	\$138	0.14	\$17	0.005	\$22.0	-3.2
	2	\$135	0.13	\$20	0.005	\$20.4	
-\$1 M	1	\$134	0.16	\$15	0.016	\$25.9	+1.0
	2	\$132	0.15	\$17	0.021	\$24.6	
-\$2 M	1	\$133	0.16	\$15	0.016	\$26.6	+2.0
	2	\$131	0.15	\$17	0.021	\$25.6	
-\$3 M	1	\$132	0.17	\$15	0.016	\$27.5	+3.3
	2	\$130	0.16	\$17	0.021	\$26.9	
-\$4 M	1	\$131	0.18	\$15	0.016	\$28.4	+4.8
	2	\$131	0.15	\$15	0.059	\$30.4	
-\$5 M	1	\$130	0.18	\$15	0.016	\$29.5	+5.9
	2	\$131	0.15	\$14	0.067	\$31.5	

The results of Table 3.9 show that in this case, the budget constraint is reasonable since small variations of the budget lead to equal variations of the expected failure costs.

3.4 Summary for Case 1

The PPRM model provides decision support for the project manager in selecting the optimal technical design alternative and level of budget reserves. When projects involve significant technical and management risks, determining the optimal alternative based on experience or intuition may be difficult. For example, single-string systems are often assumed to be the preferred alternative for Faster-Better-Cheaper projects because of the lower cost. The illustration in this chapter shows that if significant investment is required to make a single-string design sufficiently reliable, it is not necessarily preferred to a partially redundant system.

CHAPTER 4

Case 2- Single Project, Warning System Required for Problem Detection

4.1 Introduction to the PPRM Model with the Choice of a Warning System

Case 2 relaxes the assumption that problems are immediately detected when they occur. The three steps of the PPRM model described in Chapter 3 are still applicable. However, now, a warning system (i.e., a combination of testing and reviews) is required to detect problems during development. To choose a warning system, we consider the amount of project budget to be allocated to reviews and testing because these tasks are critical in the identification of potential problems in the system. The optimal selection of a warning system involves several factors:

- More investment in a warning system implies less money for development.
- More investment in a warning system generally results in a higher likelihood of detecting problems.
- Investments in warning systems have decreasing marginal returns, (i.e., there is a point when additional reviews and testing is not cost effective as the number of detected problems decreases.)

Imperfect warning systems may fail to detect existing problems. Undetected problems affect the probability of failure of the system in two ways:

- undetected problems in a particular component or subsystem increase the probability of failure of that component or subsystem, thus resulting in a higher probability of technical failure for the whole system, and
- undetected problems decrease the probability of management failure, because no resources are expended mitigating undetected problems.

The decision for the project manager is to optimally allocate the available resources above the minimum cost system for each possible design alternative among reserves, testing and reviews, and development to determine the optimal design alternative and corresponding level of warning system. This allocation decision is represented in Figure 4.1 by the adjustable divisions among the design and development budget, the warning system budget, and the reserves.

The outputs of the PPRM model for Case 2 are (1) the recommended functional design configuration and components, (2) the development budget and corresponding reserve budget, and (3) the recommended choice of warning system. Section 4.2 describes the modifications of the PPRM model needed to incorporate the potential for undetected problems, and Section 4.3 provides an illustration of the model including the choice of a warning system.

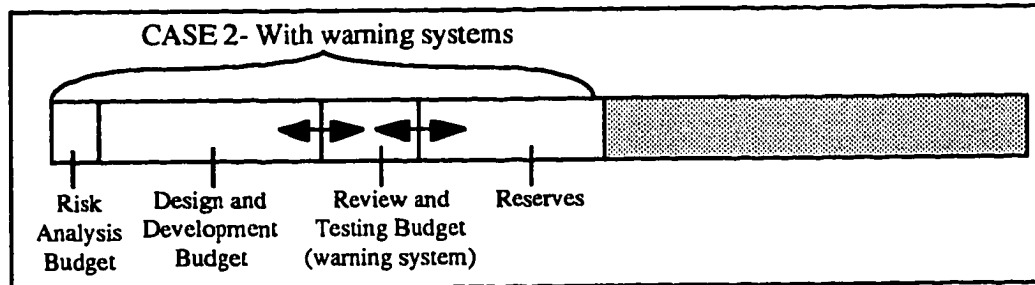


Figure 4.1- Case 2: Budget Allocation Between Development, Warning System, and Reserves

4.2 Model Revisions to Include a Choice of Warning System

The following additional notation is used in describing the PPRM model with the choice of a warning system:

- Warning system alternative, indexed in j : WS_j
- Cost of warning system alternative: $C(WS_j)$
- Undetected design problem in subsystem s : UDP_s
- No undetected design problem in subsystem s : \overline{UDP}_s
- Detected design problem in subsystem s : DDP_s
- Detected design problem scenario indexed in ℓ : $DDPS_\ell$

The following is a summary of the three steps in the PPRM model previously described in Chapter 3:

STEP 1: Develop and optimize all feasible technical design alternatives over the range of potential project development budgets to minimize each alternative's probability of technical failure.

STEP 2: For each technical design alternative, optimize the strategy to reduce management risks over the range of potential reserve budgets, where the strategy is determined by:

- the potential management problems that could occur for each technical design alternative, and
- potential mitigation actions for each management problem.

STEP 3: Determine the optimal technical design alternative and the budget reserve based on the lowest overall expected failure cost given the optimal management risk strategies for that design.

Revisions required in Step 1: Optimize technical design alternatives.

Two revisions are required to consider the choice of a warning system in Step 1:

(1) The budget surplus (step 1.7) includes the cost of the warning system:

$$\begin{aligned} \text{Budget surplus} = & \text{Portion of Budget Allocated to Design} - & (4.1) \\ & \text{Cost of Risk Analysis} - \text{Cost}(\text{AFIG}_{z,\min}) - \text{Cost of Warning System} \end{aligned}$$

(2) For a single-string subsystem, the probability of failure of the subsystem is the sum of the probability of the failure mode with and without undetected problems multiplied by the probability of the respective problems:

$$\begin{aligned} p(\text{FM}_s | \text{AFIG}_{z,w}, \text{WS}_j) = & p(\text{FM}_s | \text{UDP}_s, \text{AFIG}_{z,w}, \text{WS}_j) \times p(\text{UDP}_s | \text{AFIG}_{z,w}, \text{WS}_j) + \\ & p(\text{FM}_s | \overline{\text{UDP}}_s, \text{AFIG}_{z,w}, \text{WS}_j) \times p(\overline{\text{UDP}}_s | \text{AFIG}_{z,w}, \text{WS}_j) \end{aligned} \quad (4.2)$$

For a redundant subsystem with two components, each of which can have undetected problems, the failure of the subsystem involves all possible combinations of undetected problems in the components:

$$\begin{aligned} p(\text{FM}_s | \text{AFIG}_{z,w}, \text{WS}_j) = & \\ & p(\text{FM}_s | \text{UDP}_{1,1}, \text{UDP}_{1,2}, \text{AFIG}_{z,w}, \text{WS}_j) \times p(\text{UDP}_{1,1}, \text{UDP}_{1,2} | \text{AFIG}_{z,w}, \text{WS}_j) + \\ & p(\text{FM}_s | \overline{\text{UDP}}_{1,1}, \text{UDP}_{1,2}, \text{AFIG}_{z,w}, \text{WS}_j) \times p(\overline{\text{UDP}}_{1,1}, \text{UDP}_{1,2} | \text{AFIG}_{z,w}, \text{WS}_j) + \\ & p(\text{FM}_s | \text{UDP}_{1,1}, \overline{\text{UDP}}_{1,2}, \text{AFIG}_{z,w}, \text{WS}_j) \times p(\text{UDP}_{1,1}, \overline{\text{UDP}}_{1,2} | \text{AFIG}_{z,w}, \text{WS}_j) + \\ & p(\text{FM}_s | \overline{\text{UDP}}_{1,1}, \overline{\text{UDP}}_{1,2}, \text{AFIG}_{z,w}, \text{WS}_j) \times p(\overline{\text{UDP}}_{1,1}, \overline{\text{UDP}}_{1,2} | \text{AFIG}_{z,w}, \text{WS}_j) \end{aligned} \quad (4.3)$$

The optimization step, using the Karush-Kuhn-Tucker algorithm, is based on the probability of the failure modes conditional on the warning system (i.e., the probability of undetected problems):

$$\text{Minimize: } p(\text{TF}|\text{AFIG}_{z,w}, \text{WS}_j) = \sum_i p(\text{FM}_i|\text{AFIG}_{z,w}, \text{WS}_j) - \text{"doubles"} + \dots \quad (4.4)$$

Revisions required in Step 2: Optimize the strategy to reduce management risks.

When examining management risks, we can only correct the problems that we detect. Problems are categorized by the set $\{q_\ell\}$ of the indices of all problems that occur and are detected during the development phase, and the set $\{r_\ell\}$ of the indices of all problems that occur and are undetected during the development. Scenarios (i.e., paths in the decision tree) are now limited to detected design problem scenarios (DDPS $_\ell$). The probability of the detected design problem scenario ℓ is the product of the probabilities of development problems that occur multiplied by the probability of detection, the probabilities of development problems that occur multiplied by the probability of no detection, and the complements of the probabilities of development problems that do not occur:

$$p(\text{DDPS}_\ell|\text{WS}_j) = \prod_{m \in \{q_\ell\}} p(\text{DP}_m) \times p(\text{DDP}_m|\text{DP}_m, \text{WS}_j) \times \prod_{m \in \{r_\ell\}} p(\text{DP}_m) \times (1 - p(\text{DDP}_m|\text{DP}_m, \text{WS}_j)) \times \prod_{m \in \{q_\ell, r_\ell\}} (1 - p(\text{DP}_m)) \quad (4.5)$$

The indicator variable for the outcome, γ , is $\gamma=1$ if the optimal risk mitigation strategy for scenario ℓ , RM_ℓ^* , does not exceed cost or schedule reserves given the detected development problem scenario DDPS $_\ell$ (i.e., only detected problems can be mitigated), and $\gamma = 0$ otherwise:

$$\gamma = \begin{cases} 1, & \text{if } C(\text{RM}_\ell^*)|\text{DDPS}_\ell \leq \text{RC and } S(\text{RM}_\ell^*)|\text{DDPS}_\ell \leq \text{RS} \\ 0, & \text{otherwise management failure} \end{cases} \quad (4.6)$$

For each design alternative and choice of warning system, the probability of management failure is one minus the sum of the outcome of each detected design problem scenario as defined by the indicator variable γ multiplied by the probability of that scenario:

$$p(\text{MF}|\text{AFIG}_{z,w}, \text{WS}_j) = 1 - \sum_t (\gamma|\text{AFIG}_{z,w}, \text{DDPS}_t, \text{WS}_j) \times p(\text{DDPS}_t|\text{WS}_j). \quad (4.7)$$

When considering management failure, since we only correct the problems that we detect, warning systems that do not detect many problems are preferred from a cost reserve perspective (i.e., no problems, no costs to mitigate). The tradeoff is that these undetected problems increase the probability of technical failure. Also, we assume that warning systems do not generate false positives.

Revisions required in Step 3: Determine the optimal technical design alternative based on the lowest overall expected failure cost.

The probabilities of management failure and technical failure should reflect the revisions in the previous steps. The expected failure cost is the sum of the cost of each failure state multiplied by the probability of that state:

$$E(\text{AFIG}_{z,w}) = C(\text{MF}) \times p(\text{MF}|\text{AFIG}_{z,w}, \text{WS}_j) + C(\text{TF}) \times p(\text{TF}|\text{AFIG}_{z,w}, \text{WS}_j). \quad (4.8)$$

4.3 Illustration of the Model for Case 2

Reconsider the planetary orbiter mission examined in Case 1:

- Total budget: \$150 million (including the launch vehicle)
- Total schedule: 3 years
- Two instruments: a gamma ray spectrometer and a camera.

In Case 2, the project manager has a choice between two different warning systems:

- (1) a "perfect" warning system that detects all development problems, and costs \$2 million, and
- (2) a less than "perfect" warning system that detects many problems (but not all), and costs \$1 million.

First, we consider WS_1 , the "perfect" system. Since we are examining the same mission as was evaluated in Case 1 and the problems were detected perfectly in that case, the configurations and alternatives available are the same. The total budget, however, must also include the \$2 million for the "perfect" warning system. The optimization algorithm steps are identical to the ones outlines in Section 3.3 except that the total available budget is

\$148 million plus \$2 million for WS_1 . Table 4.1 shows the results of optimal design choices for configuration 1. The best technical design alternative for configuration 1 (i.e., the lowest achievable expected cost of failure) is obtained by spending \$133 million on development and keeping \$15 million in reserves. Table 4.2 shows the results of optimal design choices for configuration 2. The best technical design alternative for configuration 2 is obtained by spending \$131 million on development and keeping \$17 million in reserves. The development costs in both tables include \$1 million for the project risk analysis.

Table 4.1- Case 2: Design Alternatives for Configuration 1, WS_1
(Total Available Budget = \$148M + \$2M for WS_1)

Development (M)	p(TF)	Reserves (M)	p(MF)	E(Cost of Failure) (\$M)
\$138	0.142	\$10	0.164	42.4
\$137	0.145	\$11	0.124	37.6
\$136	0.149	\$12	0.055	29.3
\$135	0.154	\$13	0.055	30.0
\$134	0.159	\$14	0.034	28.1
\$133	0.164	\$15	0.016	26.6
\$132	0.170	\$16	0.016	27.5
\$131	0.176	\$17	0.005	27.0
\$130	0.184	\$18	0.003	28.0

Table 4.2- Case 2: Design Alternatives for Configuration 2, WS_1
(Total Available Budget = \$148M + \$2M for WS_1)

Development (M)	p(TF)	Reserves (M)	p(MF)	E(Cost of Failure) (\$M)
\$140	0.122	\$8	0.461	79.0
\$139	0.123	\$9	0.280	55.2
\$138	0.125	\$10	0.280	55.4
\$137	0.127	\$11	0.216	47.4
\$136	0.129	\$12	0.150	38.9
\$135	0.132	\$13	0.150	39.3
\$134	0.135	\$14	0.067	29.0
\$133	0.14	\$15	0.059	28.6
\$132	0.146	\$16	0.051	28.4
\$131	0.153	\$17	0.02	25.6

Next, we consider WS_2 , the "cheap" warning system with the potential for undetected problems. For this alternative, we need to repeat the three-step optimization algorithm.

STEP 1: Optimize technical design alternative.

Step 1.1 Identify the spacecraft functions given the scope of the mission.

Unchanged from Case 1.

Step 1.2 Identify the set of functional configurations, FIG.

Unchanged from Case 1.

Step 1.3 Define AFIG as the set of functional configurations and associated components.

Unchanged from Case 1.

Step 1.4 For each functional configuration, determine $AFIG_{z,min}$, the lowest-cost alternative.

Unchanged from Case 1.

Step 1.5 Fix the risk analysis budget and the schedule allocation.

Unchanged from Case 1.

Step 1.6 Determine the feasible subset of $\{ AFIG_{z,min} \}$.

Unchanged from Case 1.

Step 1.7 For each feasible functional configuration, vary the amount allocated to development and compute the resulting budget surplus as follows:

$$\begin{aligned} \text{Budget surplus} = & \text{Portion of Budget Allocated to Design} - & (4.9) \\ & \text{Cost of Risk Analysis} - \text{Cost}(AFIG_{z,min}) - \text{Cost of } WS_2 \end{aligned}$$

$\$0 < \text{Budget surplus for configuration 1} < \24 million

$\$0 < \text{Budget surplus for configuration 2} < \19 million

Step 1.8 Use a PRA model of the configuration and the Karush-Kuhn-Tucker algorithm to optimize the design based on the cost of improvements, the budget surplus, and associated contributions to the reduction of technical risk : $p(TF/AFIG_{z,w})$.

Configuration 1 (single-string) with "cheap" warning system (WS_2)

Table 4.3 shows the probabilities of the failure modes for the subsystems in $AFIG_{1,min}$ given no undetected problems, assuming that all basic event failures are independent. Table 4.4 shows the probabilities of the failure modes for the subsystems in $AFIG_{1,min}$ given an undetected problem in the subsystem (i.e., we assume that an undetected problem

increases the probability of failure by a factor of five). Table 4.5 shows the probability of undetected problems in each subsystem if WS₂, the "cheap" system, is implemented.

Table 4.3- Case 2: Probability of Failure Modes Given No Undetected Problems, Configuration 1, WS₂

Subsystem	$p(\text{FM}_i \overline{\text{UDP}}_s, \text{AFIG}_{1,\text{min}})$
Launch Vehicle	0.1
Communications Subsystem	0.1
Spacecraft	0.01
Instruments Package	0.05

Table 4.4- Case 2: Probability of Failure Modes Given Undetected Problems, Configuration 1, WS₂

Subsystem	$p(\text{FM}_i \text{UDP}_s, \text{AFIG}_{1,\text{min}})$
Launch Vehicle	0.5
Communications Subsystem	0.5
Spacecraft	0.05
Instruments Package	0.25

Table 4.5- Case 2: Probability of Undetected Problems, Configuration 1, WS₂

Subsystem	$p(\text{UDP}_i \text{AFIG}_{1,\text{min}}, \text{WS}_2)$
Launch Vehicle	0.0
Communications Subsystem	0.1
Spacecraft	0.5
Instruments Package	0.1

The probability of technical failure for the lowest-cost design for configuration 1 with the "cheap" warning system is:

$$\begin{aligned}
p(\text{TF}|\text{AFIG}_{\Lambda,\min}, \text{WS}_2) = & \\
& \sum_{s \in \{\text{LV}, \text{CS}, \text{SC}, \text{IS}\}} \left[p(\text{FM}_s | \text{UDP}_s, \text{AFIG}_{1,\min}, \text{WS}_2) \times p(\text{UDP}_s | \text{AFIG}_{1,\min}, \text{WS}_2) + \right. \\
& \left. p(\text{FM}_s | \overline{\text{UDP}}_s, \text{AFIG}_{1,\min}, \text{WS}_2) \times p(\overline{\text{UDP}}_s | \text{AFIG}_{1,\min}, \text{WS}_2) \right] - \quad (4.10) \\
& \text{"doubles" + ...} \\
& = 0.30
\end{aligned}$$

Repeating the optimization process from Case 1, we consider possible reductions of the probability of technical failure given investments in improvements above the minimum or cheapest components, using the data provided in Table 4.6.

Table 4.6- Case 2: Effects of Investment on Reinforcement of Configuration 1, WS₂

Subsystem	Investment	Reduction Factor
Launch Vehicle	n.a.	n.a.
Communications Subsystem	\$12M	10
Spacecraft	\$10M	10
Instruments Package	\$10M	10

Figure 4.2 shows on one y-axis, the optimal investment in each subsystem for various levels of investment, and on the second y-axis, the effect of various levels of investment on the probability of technical failure for the system. Compare Figure 4.2 and Figure 3.10. Figure 3.10 represents investments in the same configuration without the possibility of undetected problems. In both figures, the communications subsystem and the instruments receive most of the investment in reinforcement. The amount invested in the spacecraft is greater, however, in Figure 4.2. This investment is a result of the 0.5 probability of an undetected problem in that subsystem.

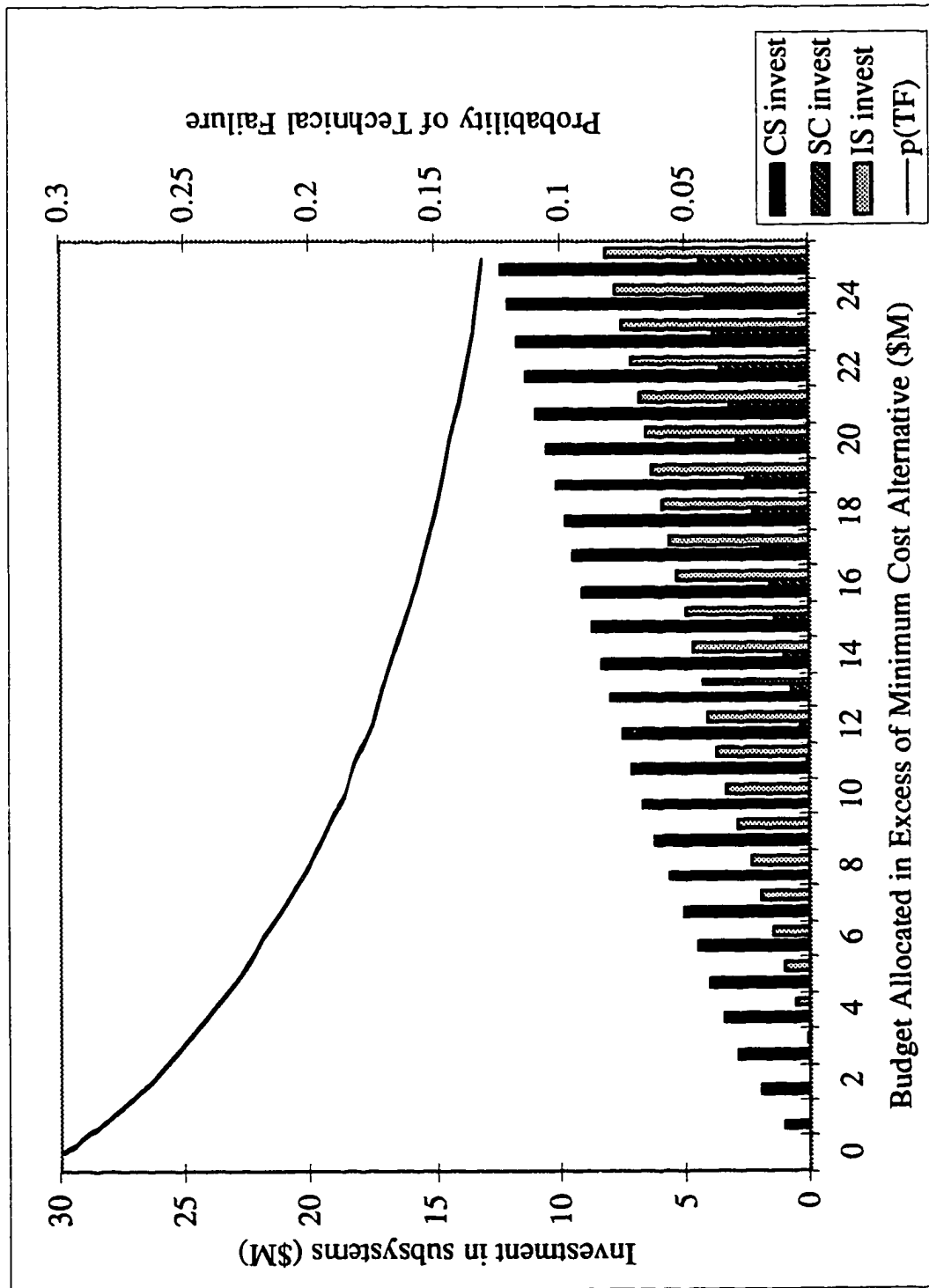


Figure 4.2- Case 2: Various Investment Levels for Configuration 1, WS₂

Configuration 2 (partially redundant) with "cheap" warning system (WS₂)

Table 4.7 shows the probabilities of the failure modes for the subsystems in AFIG_{2,min} given no undetected problems, assuming that all basic event failures are independent. Table 4.8 shows the probabilities of the failure modes for the subsystem in AFIG_{2,min} given an undetected problem in the subsystem (i.e., we assume that an undetected problem increases the probability of failure by a factor of five). Table 4.9 shows the probability of undetected problems in each subsystem if WS₂, the "cheap" system, is implemented. In this illustration, we assume independence of detected and undetected problems in subsystems and components.

Table 4.7- Case 2: Probability of Failure Modes Given No Undetected Problems, Configuration 2, WS₂

Subsystem/ Component	Subsystem Failure $p(FM_i \overline{UDP}_s, AFIG_{2,min})$
Launch Vehicle	0.1
Communications Subsystem	$p(F_{CS1} \overline{UDP}_{CS1}, AFIG_{2,min}) \times$ $p(F_{CS2} F_{CS1}, \overline{UDP}_{CS2}, AFIG_{2,min}) =$ $0.1 \times 0.1 = 0.01$
Spacecraft	0.01
Instruments Package	0.05

Table 4.8- Case 2: Probability of Failure Modes Given Undetected Problems, Configuration 2, WS₂

Subsystem/ Component	Subsystem Failure $p(FM_i UDP_s, AFIG_{2,min})$
Launch Vehicle	0.5
Communications Subsystem	$p(F_{CS1} UDP_{CS1}, AFIG_{2,min}) \times$ $p(F_{CS2} F_{CS1}, UDP_{CS2}, AFIG_{2,min}) =$ $0.5 \times 0.5 = 0.25$
Spacecraft	0.05
Instruments Package	0.25

Table 4.9- Case 2: Probability of Undetected Problems, Configuration 2, WS₂

Subsystem/ Component	Undetected Problems in Subsystem or Component $P(\text{UDP}_i \text{AFIG}_{2,\text{min}}, \text{WS}_2)$
Launch Vehicle	0.0
Communications Component 1	0.1
Communications Component 2	0.1
Spacecraft	0.5
Instruments Package	0.1

Repeating the optimization process from configuration 1, we consider possible reductions of the probability of technical failure given investments in improvements above the minimum or cheapest components, using the data provided in Table 4.10.

Table 4.10- Case 2: Effects of Investment on Reinforcement of Configuration 2, WS₂

Subsystem/ Component	Investment	Reduction Factor
Launch Vehicle	n.a.	n.a.
Communications Component 1	\$12M	10
Communications Component 2	\$12M	10
Spacecraft	\$10M	10
Instruments Package	\$10M	10

Figure 4.3 shows on one y-axis, the optimal investment in each subsystem for various levels of investment, and on the second y-axis, the effect of various levels of investment on the probability of technical failure for the system. Compare Figure 4.3 and Figure 3.11. Consistent with the observation from configuration 1, the amount invested in the spacecraft is greater in Figure 4.3. This investment is the result of the 0.5 probability of an undetected problem in that subsystem.

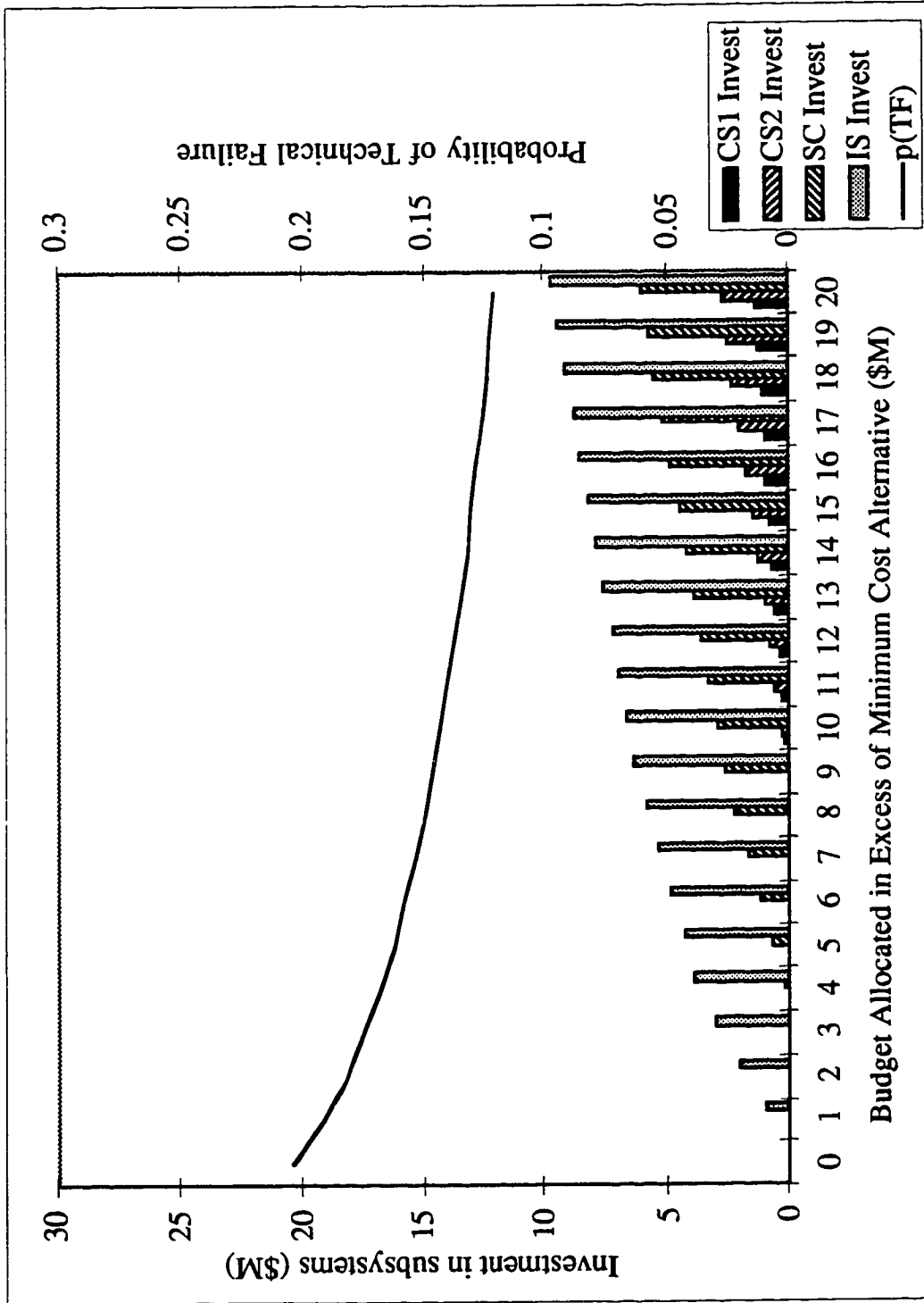


Figure 4.3- Case 2: Various Investment Levels for Configuration 2, WS₂

STEP 2: Optimize the strategy to reduce management risks.

Step 2.1 For each technical design alternative, construct development problem scenarios and possible risk mitigation responses.

Table 4.11 shows the potential problems and risk mitigation alternatives for configuration 1. Table 4.12 shows the corresponding data for configuration 2. Figure 4.4 shows a portion of the decision tree constructed from these problems and potential mitigation actions. The difference between this decision tree and the decision tree in Case 1 is the addition of chance nodes for problem detection. The preferred sequence of mitigation actions is identified with arrows. A 0 at the end of the branch denotes a management failure from either a cost or a schedule overrun, and a 1 at the end of the branch represents a successful mitigation strategy (i.e., it does not exceed the reserves).

Table 4.11- Case 2: Management Risk Data for Configuration 1, WS₂

Potential Problems conditional on technical design	Prob. of occurrence	Prob. of detection w/ WS ₂	Mitigation Alt. 1 (Solve with \$)	Mitigation Alt. 2		Other Mitigation Alt.
				(Cost)	(Sch.)	
procurement prob. (modem)	0.4	1.0	\$5 M	\$3 M	1 mo.	n.a.
software problem	0.2	1.0	\$5 M	\$3 M	1 mo.	simplify software
communications integration prob.	0.3	0.9	\$3 M	\$2 M	0.5 mo.	n.a.
insufficient test personnel	0.5	1.0	\$3 M	\$1.5 M	1 mo.	reduce testing
late instrument delivery	0.2	1.0	\$3 M	\$1.5 M	1 mo.	substitute instrument
instrument power problems	0.1	0.9	\$3 M	\$1.5 M	1 mo.	n.a.
spacecraft mass problems	0.1	1.0	\$3 M	\$2 M	1 mo.	n.a.
Unknown problems	0.5	0.5	\$5 M	\$3 M	1 mo.	n.a.

Table 4.12- Case 2: Management Risk Data for Configuration 2, WS₂

Potential Problems conditional on technical design	Prob. of occurrence	Prob. of detection w/ WS ₂	Mitigation Alt. 1 (Solve with \$)	Mitigation Alternative 2		Other Mitigation Alt.
				(Cost)	(Sch.)	
procurement prob. (modem)	0.4	1.0	\$5 M	\$3 M	1 mo.	n.a.
software problem	0.2	1.0	\$5 M	\$3 M	1 mo.	simplify software
communications integration prob.	0.6	0.9	\$5 M	\$3 M	0.5 mo.	n.a.
insufficient test personnel	0.5	1.0	\$3 M	\$1.5 M	1 mo.	reduce testing
late instrument delivery	0.2	1.0	\$3 M	\$1.5 M	1 mo.	substitute instrument
instrument power problems	0.1	0.9	\$3 M	\$1.5 M	1 mo.	n.a.
spacecraft mass problems	0.1	1.0	\$3 M	\$2 M	1 mo.	n.a.
Unknown problems	0.5	0.5	\$5 M	\$3 M	1 mo.	n.a.

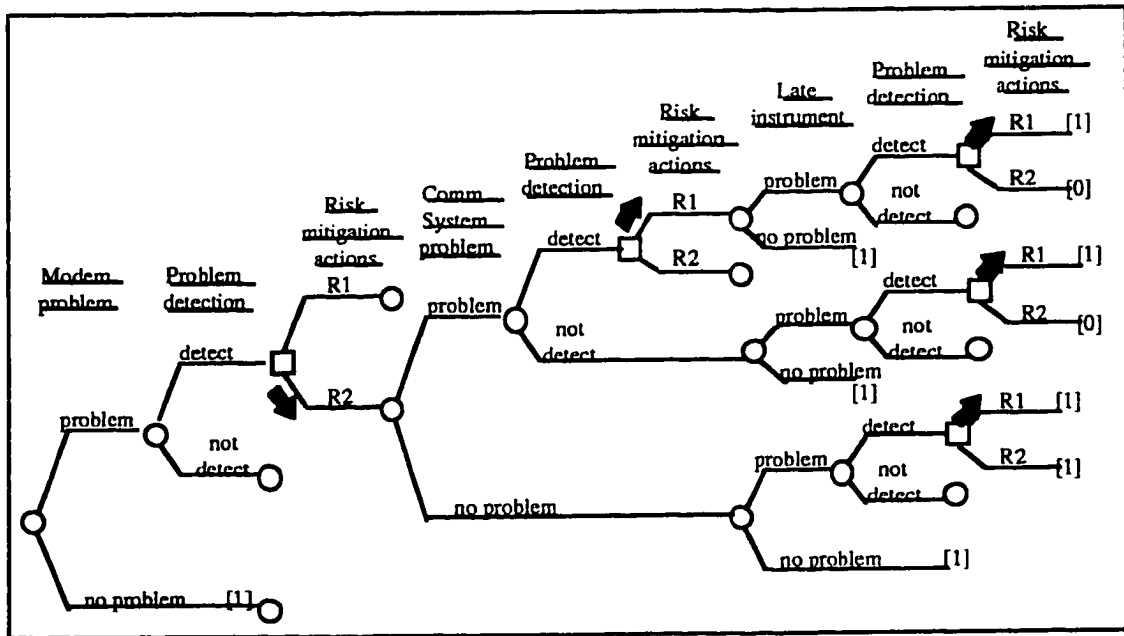


Figure 4.4- Case 2: Portion of the Decision Tree for Configuration 1, WS₂

Step 2.2 Resolve the decision tree to determine the probability of each scenario ℓ .

Completed by decision tree resolution (using Precision Tree software) [Palisade Corporation, 1997].

Step 2.3 Determine the outcome for each scenario, conditional on the optimal sequence of risk management options.

Completed by decision tree resolution (using Precision Tree software) [Palisade Corporation, 1997].

Step 2.4 For each design alternative, determine the probability of management failure given the corresponding reserves and the optimal mitigation strategy determined above.

$$p(\text{MF} | \text{AFIG}_{z,w}, \text{WS}_j) = 1 - \sum_t (\gamma | \text{AFIG}_{z,w}, \text{DDPS}_t, \text{WS}_j) \times p(\text{DDPS}_t | \text{WS}_j) \quad (4.11)$$

Figure 4.5 shows the probability of management failure as a function of the reserve allocation for both configuration 1 and configuration 2.

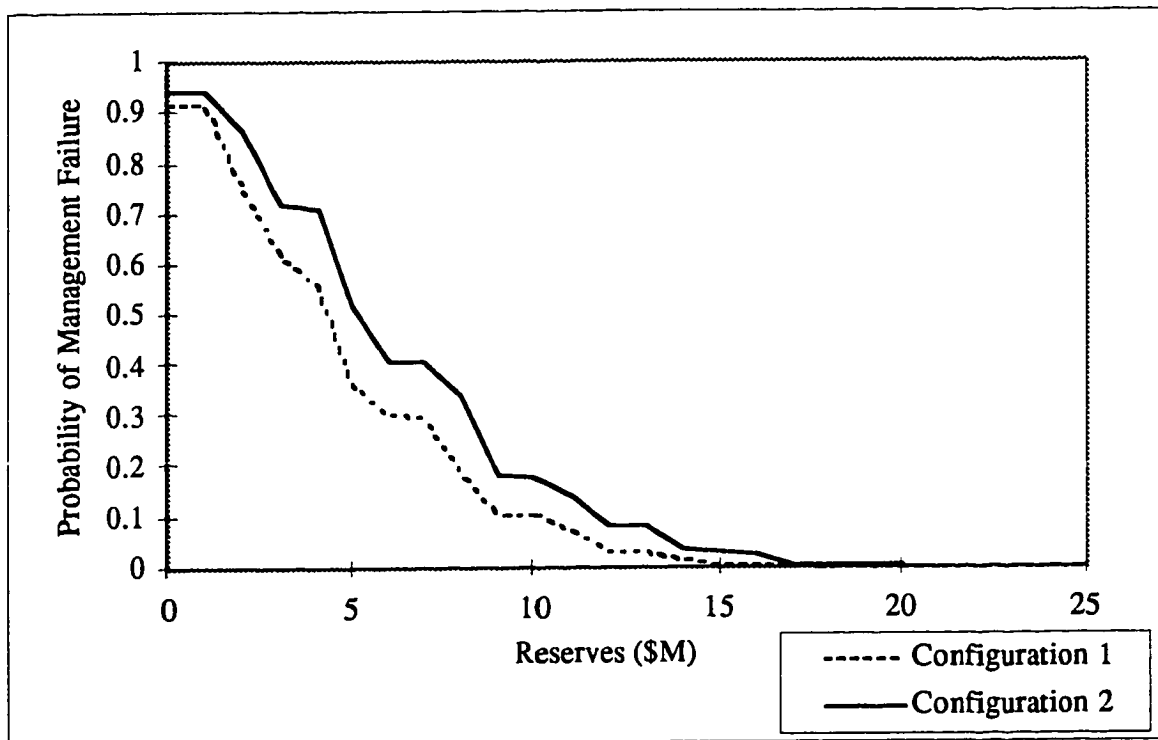


Figure 4.5- Case 2: Probability of Management Failure as a Function of the Reserve Allocation for Configurations 1 and 2, WS_2

Compare Figure 4.5 and Figure 3.13. Figure 3.13 represents the probability of management failure as a function of the reserves assuming no undetected problems. The probability of management failure is lower for all levels of reserve in Figure 4.5 than in Figure 3.13. This is because less reserves are required since not all problems are detected.

STEP 3: Determine the optimal technical design alternative based on the lowest overall expected failure cost.

Step 3.1 For each alternative, $AFIG_{z,w}$, compute the overall expected failure cost:

$$E(AFIG_{z,w}) = C(MF) \times p(MF/AFIG_{z,w}, WS_j) + C(TF) \times p(TF/AFIG_{z,w}, WS_j). \quad (4.12)$$

Assume that the Cost(TF) is \$150 M, and that the Cost(MF) is \$150 M. Table 4.13 shows the results of optimal design choices for configuration 1. The best technical design alternative for configuration 1 (i.e., the lowest achievable expected cost of failure) is obtained by spending \$134 million on development and keeping \$15 million in reserves. Table 4.14 shows the results of optimal design choices for configuration 2. The best technical design alternative for configuration 2 is obtained by spending \$132 million on development and keeping \$17 million in reserves. The development costs in both tables include \$1 million for the project risk analysis.

Table 4.13- Case 2: Design Alternatives for Configuration 1, WS_2
(Total Available Budget = \$149M + \$1M for WS_2)

Development (M)	p(TF)	Reserves (M)	p(MF)	E(Cost of Failure) (\$M)
\$139	0.17	\$10	0.106	38.3
\$138	0.17	\$11	0.073	34.8
\$137	0.18	\$12	0.030	30.3
\$136	0.18	\$13	0.030	31.0
\$135	0.19	\$14	0.018	30.4
\$134	0.19	\$15	0.008	30.0
\$133	0.20	\$16	0.008	31.2
\$132	0.21	\$17	0.003	31.8
\$131	0.22	\$18	0.001	33.0
\$130	0.23	\$19	0.001	34.4

Table 4.14- Case 2: Design Alternatives for Configuration 2, WS_2
(Total Available Budget = \$149M + \$1M for WS_2)

Development (M)	p(TF)	Reserves (M)	p(MF)	E(Cost of Failure) (\$M)
\$139	0.15	\$10	0.183	45.4
\$138	0.15	\$11	0.141	40.4
\$137	0.15	\$12	0.086	33.9
\$136	0.16	\$13	0.086	34.6
\$135	0.16	\$14	0.038	29.0
\$134	0.17	\$15	0.031	29.0
\$133	0.17	\$16	0.027	29.5
\$132	0.18	\$17	0.010	28.5
\$131	0.19	\$18	0.010	29.8
\$130	0.20	\$19	0.004	31.1

Step 3.2 Determine the optimal design alternative.

Compare the optimal design alternative for each configuration and choice of warning system (Tables 4.1, 4.2, 4.13, and 4.14). In this illustration, the rank order of alternatives based on the minimization of expected costs of failure, is as follows:

- Configuration 2 with “perfect” warning system, WS_1 : The expected cost of failure is \$25.6 million. The development budget is \$131 million (including \$1 million for risk analysis). The reserve budget is \$17 million, and the warning system costs \$2 million.
- Configuration 1 with “perfect” warning system, WS_1 : The expected cost of failure is \$26.6 million. The development budget is \$133 million (including \$1 million for risk analysis). The reserve budget is \$15 million, and the warning system costs \$2 million.
- Configuration 2 with “cheap” warning system, WS_2 : The expected cost of failure is \$28.5 million. The development budget is \$132 million (including \$1 million for risk analysis). The reserve budget is \$17 million, and the warning system costs \$1 million.
- Configuration 1 with “cheap” warning system, WS_2 : The expected cost of failure is \$30.0 million. The development budget is \$134 million (including \$1 million for risk analysis). The reserve budget is \$15 million, and the warning system costs \$1 million.

For both configurations, the more expensive warning system is preferred because of the significant contribution of undetected problems to the probability of technical failure. This probability of technical failure for each development alternative shown in Table 4.14 (the “cheap” warning system) is 0.03 to 0.05 greater than the equivalent probability of technical failure shown in Table 4.2 (the “perfect” warning system). While the probability of management failure is smaller for the imperfect warning system, the decrease is not large enough to offset the increase of technical risks. The preferred alternative is also highly dependent on the additional costs of the “perfect” warning system. If the costs were \$5 million rather than \$2 million, the imperfect system would be preferred.

4.4 Summary for Case 2

The PPRM model provides decision support for managers choosing a project warning system (level of testing and project reviews) and selecting the optimal technical design alternative. The illustration presented in this chapter shows that investing in a more reliable warning system can be preferred if problems are detectable at a reasonable cost and if significant technical failure risks exist from undetected problems in the system. There is a point, however, where the costs of a more reliable warning system are too large, and where the money may be better spent reinforcing the system or solving management problems.

CHAPTER 5

Case 3- Single Project with Partial Failures

5.1 Introduction to the PPRM Model with Partial Failures

Case 3 relaxes the assumption in Case 2 that all failures result in the total loss of the mission. The three steps of the PPRM model described in previous chapters are still applicable. However, additional outcome states of partial failures are now included. The outputs of the PPRM model are the same as for Case 2: (1) the recommended functional design configuration and components, (2) the development budget and corresponding reserve budget, and (3) the recommended choice of warning system. The difference between Case 2 and Case 3 is that the Case 3 analysis includes the effects of two types of partial failures: partial management failure (PMF) and partial technical failure (PTF). An example of a partial management failure is a reduction in the scope of the project (“descope”) where a new technology component is replaced with an already existing one. A partial technical failure is the failure of a part of the system that degrades but does not cease spacecraft operations.

When considering partial failures, the decision maker needs to consider how much of a “failure” is a partial failure? For example, if the project needs to descope an instrument, is the project 20% successful or 80%?

For simplicity, we assume that a partial management failure does not alter either the probability of technical failure nor the probability of partial technical failure. This assumption may need to be reevaluated in cases where the probability of a partial management failure is sufficiently large or where a descope significantly affects the reliability of the system.

Section 5.2 describes revisions to the PPRM model for incorporating partial failures, and Section 5.3 provides an illustration of the model.

5.2 Model Revisions to Include Partial Failures

The following is a summary of the three steps in the PPRM model described previously:

STEP 1: Develop and optimize all feasible technical design alternatives over the range of potential project development budgets to minimize each alternative's probability of technical failure.

STEP 2: For each technical design alternative, optimize the strategy to reduce management risks over the range of potential reserve budgets, where the strategy is determined by:

- the potential management problems that could occur for each technical design alternative, and
- potential mitigation actions for each management problem.

STEP 3: Determine the optimal technical design alternative and budget reserve based on the lowest overall expected failure cost given the optimal management risk strategies for that design.

Revisions required in Step 1: Optimize technical design alternatives.

The optimization step, using the Karush-Kuhn-Tucker algorithm, that previously considered only the probability of the failure modes conditional on the warning system, must now include the probability of partial technical failures:

$$\text{Minimize: } p(\text{TF}|\text{AFIG}_{z,w}, \text{WS}_j) + k_1 p(\text{PTF}_1|\text{AFIG}_{z,w}, \text{WS}_j) + k_2 p(\text{PTF}_2|\text{AFIG}_{z,w}, \text{WS}_j) + \dots \quad (5.1)$$

where the k_1 and k_2 are constants that represent the decision maker's valuation of a partial technical failure (as compared to a complete technical failure) for the mission.

Revisions required in Step 2: Optimize the strategy to reduce management risks.

The definition of a management failure is unchanged. Management failure occurs when the project exceeds the cost or schedule reserves. The probability of management failure is (as defined previously):

$$p(\text{MF}|\text{AFIG}_{z,w}, \text{WS}_j) = 1 - \sum_t (\gamma|\text{AFIG}_{z,w}, \text{DDPS}_t, \text{WS}_j) \times p(\text{DDPS}_t|\text{WS}_j), \text{ where} \quad (5.2)$$

$$\gamma = \begin{cases} 1, & \text{if } C(\text{RM}^*_t)|\text{DDPS}_t \leq \text{RC and } S(\text{RM}^*_t)|\text{DDPS}_t \leq \text{RS} \\ 0, & \text{otherwise management failure} \end{cases} \quad (5.3)$$

The partial management failure is a project success where success was obtained only by descoping a component. Specifically, a partial management failure occurs when cost and schedule reserves are not exceeded, but a descope was required to avoid exhausting the reserves. This case is represented by $\lambda = 1$ in the following equation:

$$\lambda = \begin{cases} 1, & \text{if } C(RM_i^*) \leq RC \text{ and } S(RM_i^*) \leq RS \text{ with a descope} \\ 0, & \text{otherwise} \end{cases} \quad (5.4)$$

The probability of partial management failure is then:

$$p(\text{PMF} | \text{AFIG}_{z,w}, WS_j) = \sum_i (\lambda_i | \text{AFIG}_{z,w}, DDPS_i, WS_j) \times p(DDPS_i | WS_j) \quad (5.5)$$

Figure 5.1 shows the development problem scenarios and mitigation responses in a decision tree, where the possible outcome states are either management success, partial management failure, or management failure. The variable d is a constant that represents the decision maker's concern for (valuation of) a partial management failure as compared to a total management failure, ($0 \leq d \leq 1$).

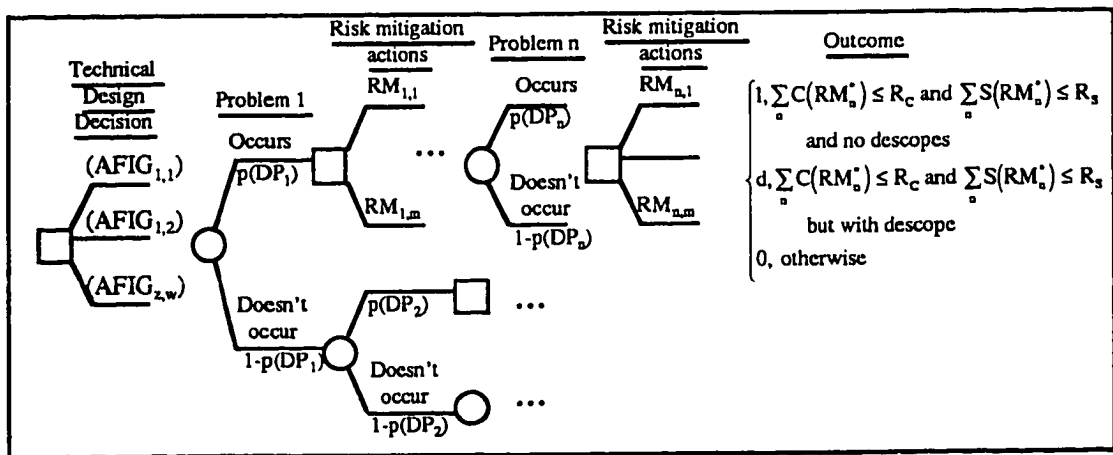


Figure 5.1- Case 3: Example Decision Tree with Partial Management Failures

Revisions required in Step 3: Determine the optimal technical design alternative based on the lowest overall expected failure cost.

The expected failure cost is the sum of the cost of each failure state multiplied by the probability of that state, assuming that a successful project outcome state has zero failure costs. All outcome states and the decision maker's preferences for each state need to be included as shown in Figure 5.2.

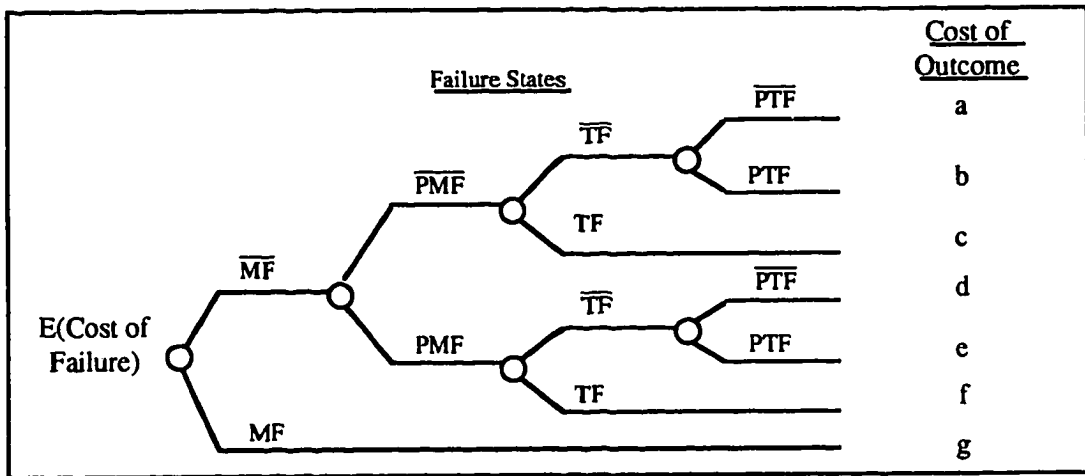


Figure 5.2- Possible Outcome States Including Partial Failures

5.3 Illustration of the Model for Case 3

Consider the mission examined in Case 2. We assume that the decision previously analyzed to invest \$2 million in the warning system (WS_1) is still valid and is not reexamined here. In this case, three partial failure modes are included. The project can result in:

- (1) a partial technical failure state, PTF_1 , if the mission loses the camera,
- (2) a partial technical failure state, PTF_2 , if the mission loses the spectrometer, and
- (3) a partial management failure state, PMF , if the managers are forced to replace the camera with a previously developed one.

The optimization process is repeated to include the additional failure states. The functional configurations from Case 2 are the same: a single-string design (configuration 1) and a design with a redundant communications subsystem (configuration 2).

STEP 1: Optimize technical design alternative.

Step 1.1 Identify the spacecraft functions given the scope of the mission.

Unchanged from previous case.

Step 1.2 Identify the set of functional configurations, FIG.

Unchanged from previous case.

Step 1.3 Define AFIG as the set of functional configurations and associated components.

Unchanged from previous case.

Step 1.4 For each functional configuration, determine $AFIG_{z,min}$, the lowest-cost alternative.

Unchanged from previous case.

Step 1.5 Fix the risk analysis budget and the schedule allocation.

Unchanged from previous case.

Step 1.6 Determine the feasible subset of $\{AFIG_{z,min}\}$.

Unchanged from previous case.

Step 1.7 For each feasible functional configuration, vary the amount allocated to development and compute the resulting budget surplus as follows:

$$\text{Budget surplus} = \text{Portion of Budget Allocated to Design} - \text{Cost of Risk Analysis} - \text{Cost}(AFIG_{z,min}) - \text{Cost of } WS_1 \quad (5.6)$$

\$0 < Budget surplus for configuration 1 < \$23 million

\$0 < Budget surplus for configuration 2 < \$18 million

Step 1.8 Use a PRA model of the configuration and the Karush-Kuhn-Tucker algorithm to optimize the design based on the cost of improvements, the budget surplus, and associated contributions to the reduction of technical risk for both complete and partial technical failures:

$$p(TF|AFIG_{z,w}, WS_1) + k_1 p(PTF_1|AFIG_{z,w}, WS_1) + k_2 p(PTF_2|AFIG_{z,w}, WS_1) + \dots \quad (5.7)$$

For each configuration 1 and 2, we assume that the probability of the technical failure modes ($p(FM_i|AFIG_{z,w})$) is unchanged from the previous case, and that the probability of any partial management failure is low enough to assume no significant effect on the probability of technical failure. In the previous case, we examined the probability of the instruments as a package ($p(FM_{IS}|AFIG_{z,w})$), where technical failure of the instrument package implied that both instruments had failed. Now, the partial failure of one instrument needs to be considered when deciding how to optimally invest any budget for the reinforcement of the system. Figure 5.3 shows the two instruments for the mission.

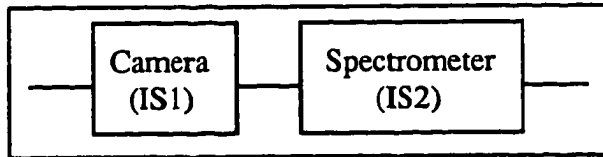


Figure 5.3- Case 3: Instrument Package

The probability of total failure of the instrument package is:

$$p(FM_{IS}|AFIG_{z,w}) = p(F_{IS1}|AFIG_{z,w}) \times p(F_{IS2}|F_{IS1}, AFIG_{z,w}). \quad (5.8)$$

The probability of failure of the camera only is:

$$p(PTF1|AFIG_{z,w}) = p(F_{IS1}, \overline{F_{IS2}}). \quad (5.9)$$

The probability of failure of the spectrometer only is:

$$p(PTF2|AFIG_{z,w}) = p(\overline{F_{IS1}}, F_{IS2}). \quad (5.10)$$

Assume that the project manager considers a mission with only a working camera 80% successful, and a mission with only a working spectrometer 40% successful. Also assume that the probability of failure of the minimum-cost components are:

$$p(F_{IS1}|AFIG_{z,min}) = 0.1 \quad (5.11)$$

$$p(F_{IS2}|AFIG_{z,min}) = 0.5 \quad (5.12)$$

Configuration 1 (single-string) with "perfect" warning system (WS₁)

Table 5.1 shows the probabilities of the failure modes for the subsystems in AFIG_{1,min}, assuming that all basic event failures are independent.

Table 5.1- Case 3: Probability of Failure Modes, Configuration 1, WS₁

Subsystem	$p(FM_i AFIG_{1,min})$
Launch Vehicle	0.1
Communications Subsystem	0.1
Spacecraft	0.01
Instruments Package	0.05

Repeating the optimization process of previous cases, we consider possible reductions of the probability of technical failure given investments in improvements above the minimum or cheapest components, using the data provided in Table 5.2.

Table 5.2- Case 3: Effects of Investment on Reinforcement of Configuration 1, WS₁

Subsystem/ Component	Investment	Reduction Factor
Launch Vehicle	n.a.	n.a.
Communications Subsystem	\$12M	10
Spacecraft	\$10M	10
Camera (IS1)	\$10M	10
Gamma Ray Spectrometer (IS2)	\$10M	10

Figure 5.4 shows the optimal investment in each subsystem for various levels of investment for configuration 1. Figure 5.5 shows the effect of various levels of investment on the probability of technical failure, the partial failure of the camera (PTF1), and the partial failure of the spectrometer (PTF2) for configuration 1. The initial increase in the probability of the partial technical failure of the camera is a result of reinforcing the spectrometer to reduce the probability of total failure of the instrument package and specifically the partial failure of the spectrometer. Reinforcement of the spectrometer results in a shift of the probability of failure of the instrument package from a total technical failure to a partial technical failure of just the camera. From Figure 5.4, for investments greater than \$4 million, a portion of that amount is spent for the reinforcement of the camera, and the probability of partial technical failure of the camera decreases. Figure 5.6 shows the optimal investment in each subsystem for various levels of investment for configuration 2, and Figure 5.7 shows the effect of various levels of investment on the probability of technical failure, the partial failure of the camera (PTF1), and the partial failure of the spectrometer (PTF2) for configuration 2.

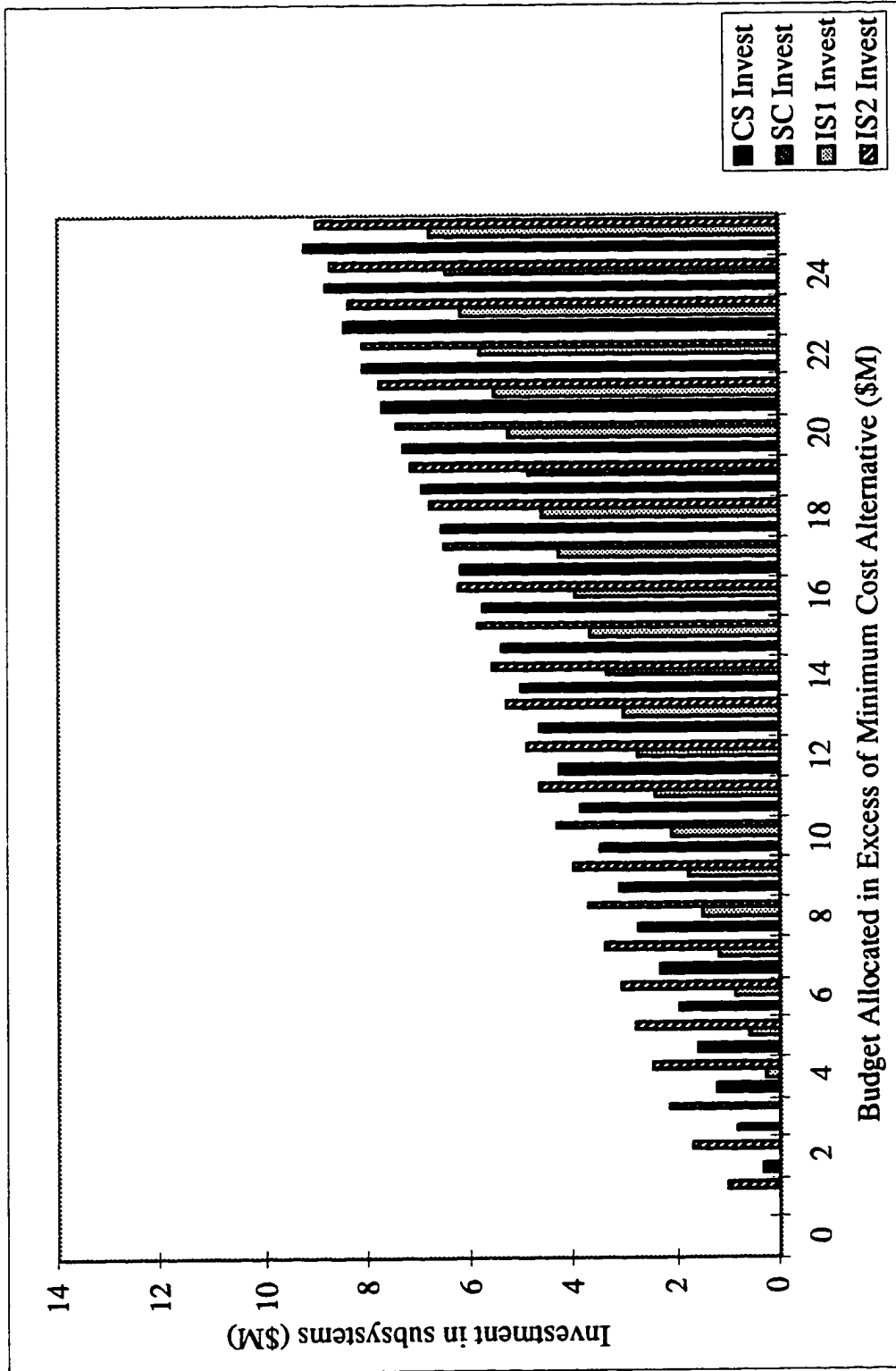


Figure 5.4- Case 3: Various Investment Levels for Configuration 1, WS₁

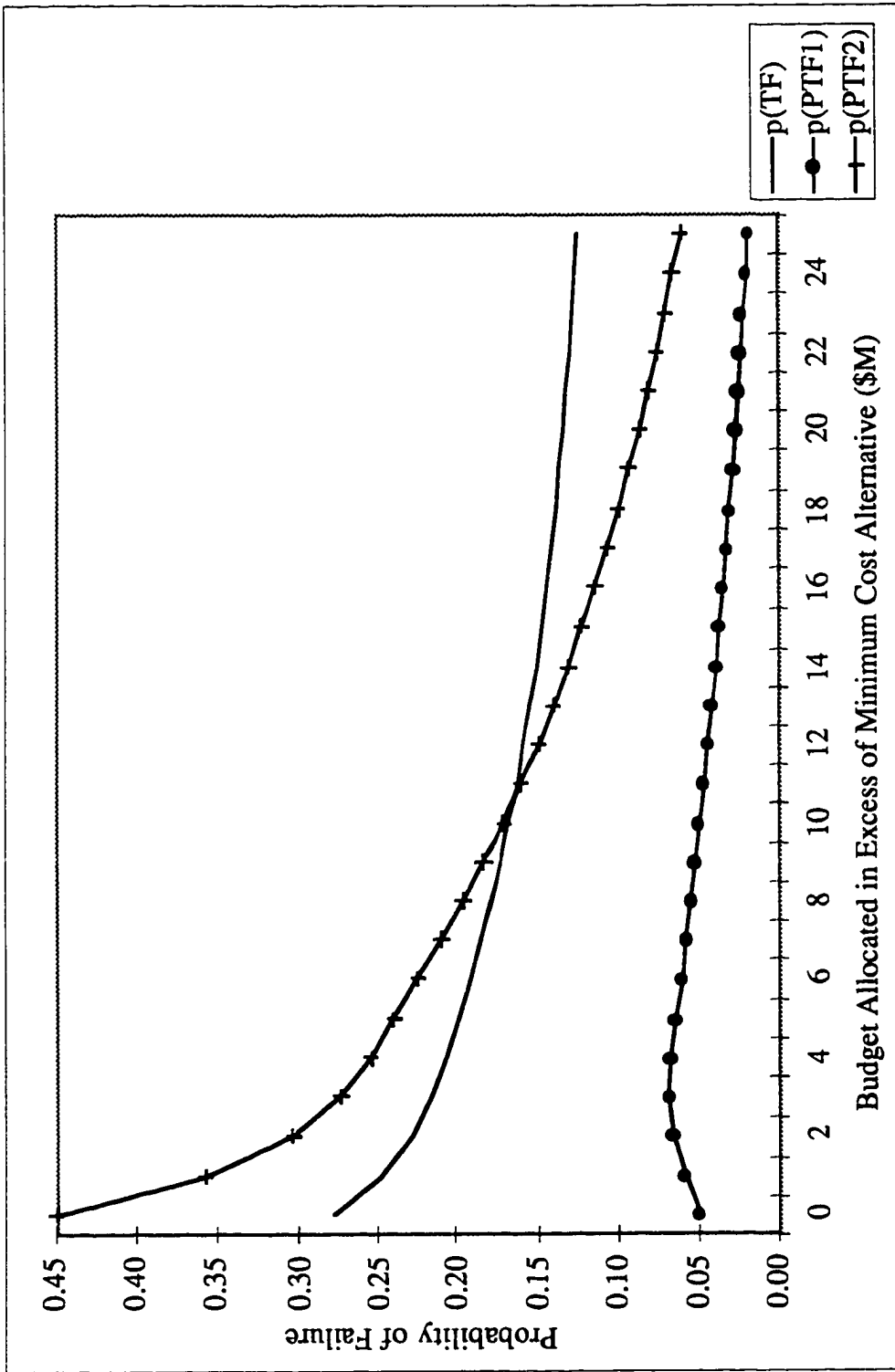


Figure 5.5- Case 3: Probability of Failure States for Various Investment Levels for Configuration 1, WS₁

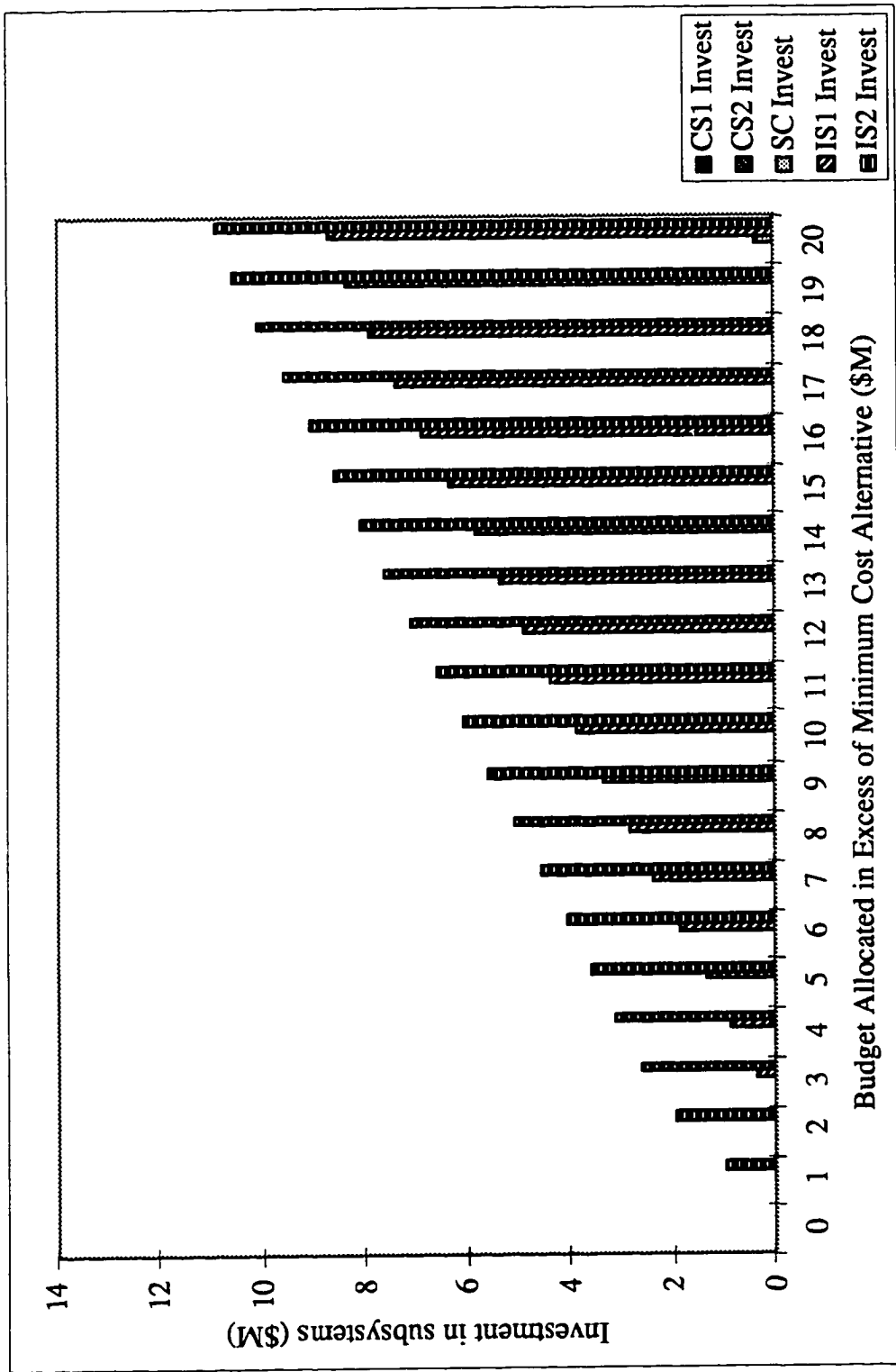


Figure 5.6- Case 3: Various Investment Levels for Configuration 2, WS₁

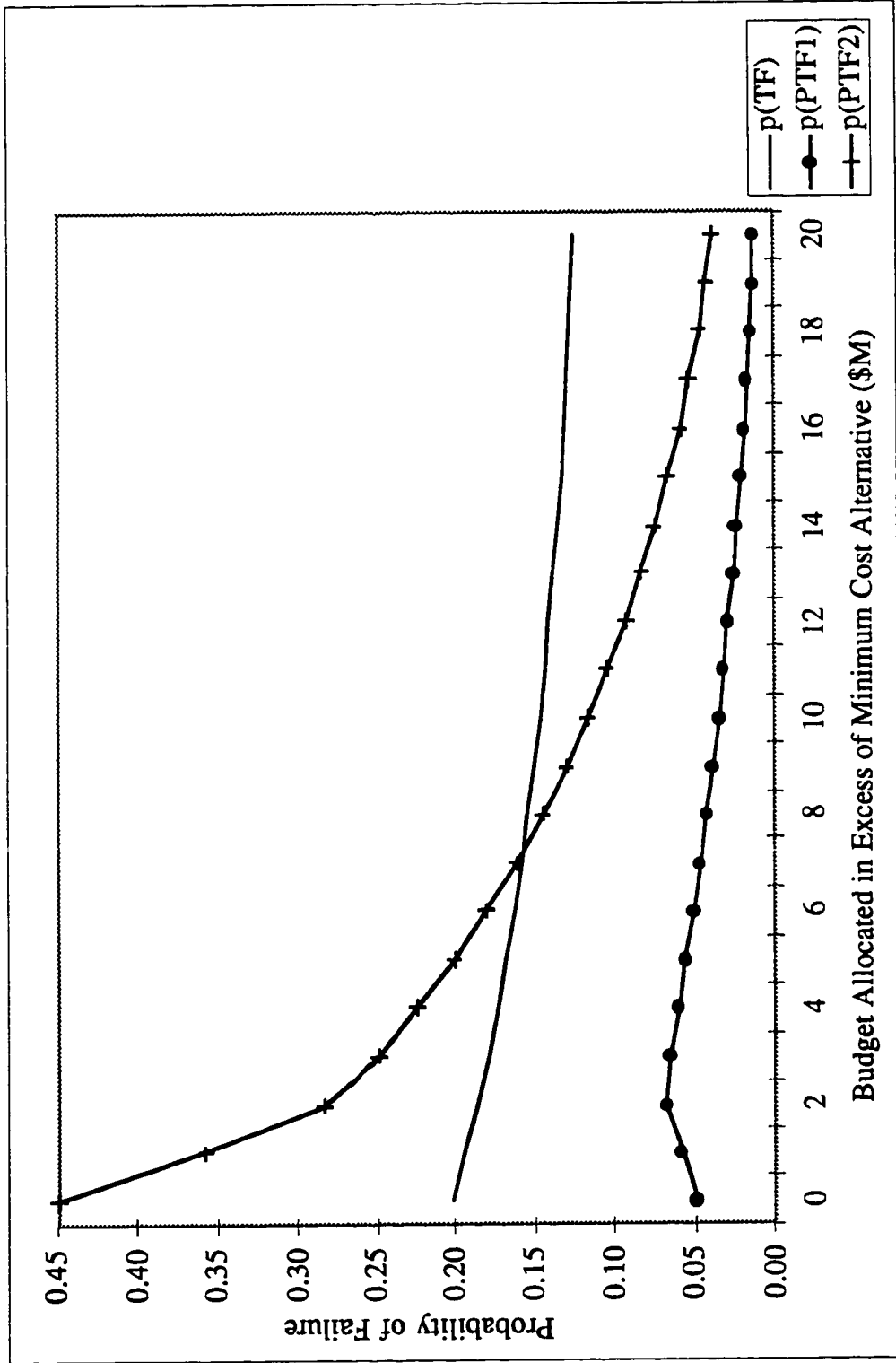


Figure 5.7- Case 3: Probability of Failure States for Various Investment Levels for Configuration 2, WS₁

STEP 2: Optimize the strategy to reduce management risks.

Step 2.1 For each technical design alternative, construct development problem scenarios and possible risk mitigation responses.

The problems and mitigation solutions previously identified remain the same. In this case, we consider the alternative mitigation strategy to substitute a spare (thus incurring no cost in terms of budget or time for a late instrument). Table 5.3 shows the potential problems and risk mitigation alternatives for configuration 1. Table 5.4 shows the corresponding data for configuration 2.

Table 5.3- Case 3: Management Risk Data for Configuration 1, WS₁

Potential Problems conditional on technical design	Probability	Mitigation Alt. 1 (Solve with \$)	Mitigation Alternative 2		Other Mitigation Alt.
			(Cost)	(Sch.)	
procurement prob. (modem)	0.4	\$5 M	\$3 M	1 mo.	n.a.
software problem	0.2	\$5 M	\$3 M	1 mo.	simplify software
communications integration prob.	0.3	\$3 M	\$2 M	0.5 mo.	n.a.
insufficient test personnel	0.5	\$3 M	\$1.5 M	1 mo.	reduce testing
late camera delivery	0.2	\$3 M	\$1.5 M	1 mo.	substitute spare
instrument power problems	0.1	\$3 M	\$1.5 M	1 mo.	n.a.
spacecraft mass problems	0.1	\$3 M	\$2 M	1 mo.	n.a.
Unknown problems	0.5	\$5 M	\$3 M	1 mo.	n.a.

Table 5.4- Case 3: Management Risk Data for Configuration 2, WS₁

Potential Problems conditional on technical design	Probability	Mitigation Alt. 1 (Solve with \$)	Mitigation Alternative 2		Other Mitigation Alt.
			(Cost)	(Sch.)	
procurement prob. (modem)	0.4	\$5 M	\$3 M	1 mo.	n.a.
software problem	0.2	\$5 M	\$3 M	1 mo.	simplify software
communications integration problem	0.6	\$5 M	\$3 M	0.5 mo.	n.a.
insufficient test personnel	0.5	\$3 M	\$1.5 M	1 mo.	reduce testing
late camera delivery	0.2	\$3 M	\$1.5 M	1 mo.	substitute spare
instrument power problems	0.1	\$3 M	\$1.5 M	1 mo.	n.a.
spacecraft mass problems	0.1	\$3 M	\$2 M	1 mo.	n.a.
Unknown problems	0.5	\$5 M	\$3 M	1 mo.	n.a.

Step 2.2 Resolve the decision tree to determine the probability of each scenario ℓ .

Completed by decision tree resolution (using Precision Tree software) [Palisade Corporation, 1997].

Step 2.3 Determine the outcome for each scenario, conditional on the optimal sequence of risk management options.

Completed by decision tree resolution (using Precision Tree software) [Palisade Corporation, 1997].

Step 2.4 For each design alternative, determine the probability of management failure and the probability of partial management failure given the corresponding reserves and the optimal mitigation strategy determined above.

Allowing management to switch instruments if it helps avoid cost and schedule overruns results in the probabilities of total and partial management failures shown in Figure 5.8. As the probability of total management failure decreases, the probability of partial management failure initially increases. The reason for this initial increase is that with too few reserves, even a descope can not prevent total management failure. With reserves of \$6 million, the project can avoid a total management failure with probability 0.06 by substituting the spare

instrument. As reserves increase beyond \$6 million and the probability of management failure declines, the descope alternative becomes less necessary.

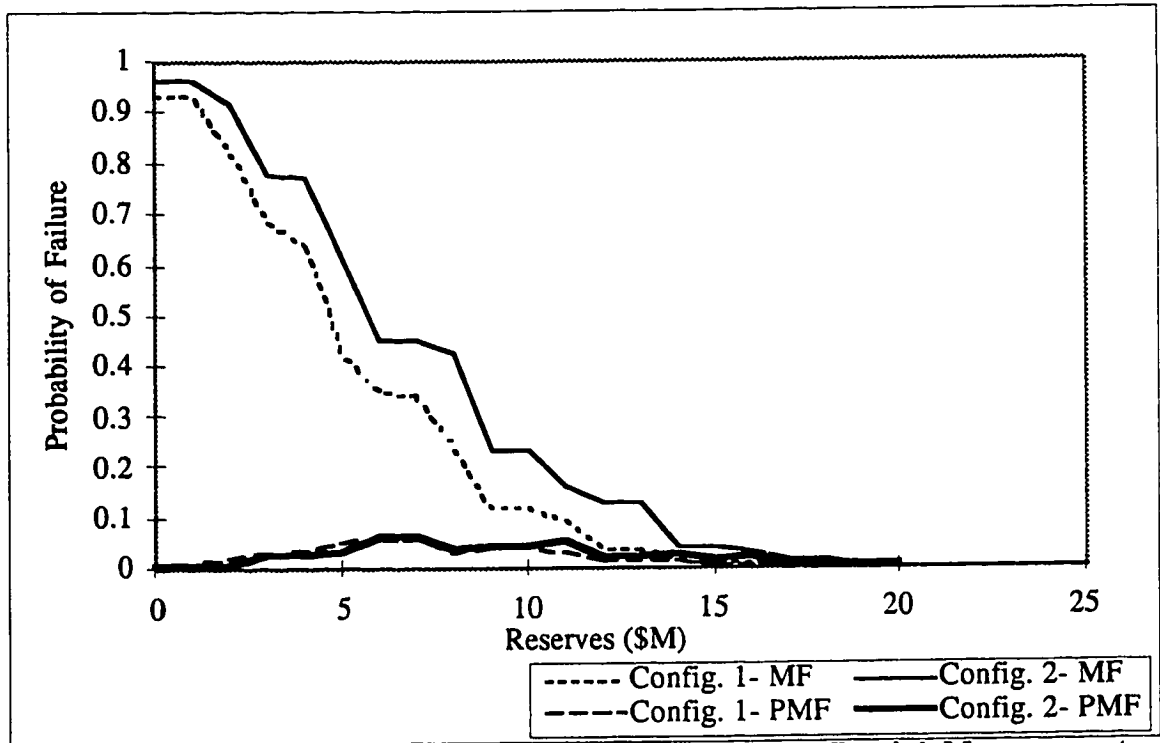


Figure 5.8- Case 3: Probability of Management and Partial Management Failure as a Function of the Reserve Allocation for Configurations 1 and 2, WS_1

STEP 3: Determine the optimal technical design alternative based on the lowest overall expected failure cost

Step 3.1 For each alternative, $AFIG_{i,w}$ and the corresponding remaining budget reserve, compute the overall expected failure cost.

Assume the following costs of failure:

- $C(TF) = \$150 \text{ M}$
- $C(MF) = \$150 \text{ M}$
- $C(PMF) = \$90 \text{ M}$
- $C(PTF1) = \$90 \text{ M}$
- $C(PTF2) = \$30 \text{ M}$
- $C(PMF,PTF1) = \$90\text{M}$

- $C(\text{PMF}, \text{PTF2}) = \90 M

These costs of failure represent the decision maker's preferences for a partial failure versus a total failure of the mission.

Table 5.5 shows the results of optimal design choices for configuration 1. The best technical design alternative for configuration 1 (i.e., the lowest achievable expected cost of failure) is obtained by spending \$133 million on development and keeping \$15 million in reserves. Table 5.6 shows the results of optimal design choices for configuration 2. The best technical design alternative for configuration 2 is obtained by spending \$134 million on development and keeping \$14 million in reserves. The development costs in both tables include \$1 million for the project risk analysis.

Table 5.5- Case 3: Design Alternatives for Configuration 1, WS_1
(Total Available Budget = \$148M + \$2M for WS_1)

Development (M)	p(TF)	p(PTF1)	p(PTF2)	Reserves (M)	p(MF)	p(PMF)	E(Cost of Failure) (\$M)
\$138	0.152	0.042	0.141	\$10	0.120	0.044	47.5
\$137	0.155	0.045	0.151	\$11	0.094	0.030	44.2
\$136	0.159	0.047	0.161	\$12	0.038	0.016	37.5
\$135	0.164	0.050	0.173	\$13	0.038	0.016	38.5
\$134	0.169	0.053	0.184	\$14	0.019	0.015	37.3
\$133	0.174	0.056	0.197	\$15	0.010	0.006	36.8
\$132	0.180	0.059	0.210	\$16	0.010	0.006	38.1
\$131	0.186	0.062	0.225	\$17	0.002	0.003	38.4
\$130	0.193	0.065	0.240	\$18	0.001	0.002	39.7

Table 5.6- Case 3: Design Alternatives for Configuration 2, WS_1
(Total Available Budget = \$148M + \$2M for WS_1)

Development (M)	p(TF)	p(PTF1)	p(PTF2)	Reserves (M)	p(MF)	p(PMF)	E(Cost of Failure) (\$M)
\$140	0.122	0.036	0.117	\$8	0.424	0.037	79.5
\$139	0.123	0.040	0.131	\$9	0.236	0.044	57.5
\$138	0.125	0.043	0.146	\$10	0.236	0.044	58.2
\$137	0.127	0.048	0.163	\$11	0.164	0.052	51.1
\$136	0.129	0.052	0.182	\$12	0.128	0.022	45.5
\$135	0.132	0.057	0.202	\$13	0.128	0.022	46.6
\$134	0.135	0.062	0.224	\$14	0.043	0.024	38.1
\$133	0.140	0.066	0.249	\$15	0.041	0.017	38.9
\$132	0.146	0.068	0.284	\$16	0.032	0.019	39.7
\$131	0.153	0.060	0.357	\$17	0.015	0.006	38.8

The recommendation for this illustration is to choose the single-string system, invest \$133 million in development and keep \$15 million in reserves. The development includes investments above the minimum of \$2.8 million in the communications system, \$1.5 in instrument 1 (camera), and \$3.7 million in instrument 2 (spectrometer).

The shift to the single-string design results from the additional penalty for a partial technical failure from the failure of an instrument. Compare this preferred alternative to the optimal design alternative for configuration 2 in Case 2 (with the equivalent warning system). Without partial failures, the preferred alternative was configuration 2 with an investment of \$131 million in development and \$17 million in reserves (Table 4.2). With partial failures, the best alternative for configuration 2 shifts an additional \$3 million from the reserve budget to the development budget. Because these additional resources are required to reinforce the instrument package, configuration 1, the simpler single-string design is preferred.

5.4 Summary for Case 3

Case 3 introduced several additional failure states into the PPRM model. These partial failures can be both managerial (e.g., descoping a project) and technical (failure of some component only). To account for these partial failure states, the decision maker needs to provide his preferences for how much of a "failure" is a partial failure. If the cost impact of the partial failure state is significant, as was the case in the illustration for the loss of the camera, partial failures can affect the preferred alternative by shifting budget resources to development in order to strengthen the design.

CHAPTER 6

Case 4- Dependent Projects in a Program

6.1 Introduction to the PPRM Model for Dependent Projects in a Program

In programs, the results of earlier projects can influence the development and success of subsequent projects, and thus managers of one project should consider the impacts of their decisions on future projects. Case 4 is an extension of the previous cases to analyze a program of two projects. The decisions of the manager of project 1 are based on an optimal allocation of the available resources above the minimum cost for each possible configuration. The resources are allocated among reserves, testing and reviews, and development, to determine the optimal design alternative, budget reserves, and corresponding level of warning system, while considering the impact of the possible outcomes of project 1 on project 2. These management decisions are represented in Figure 6.1.

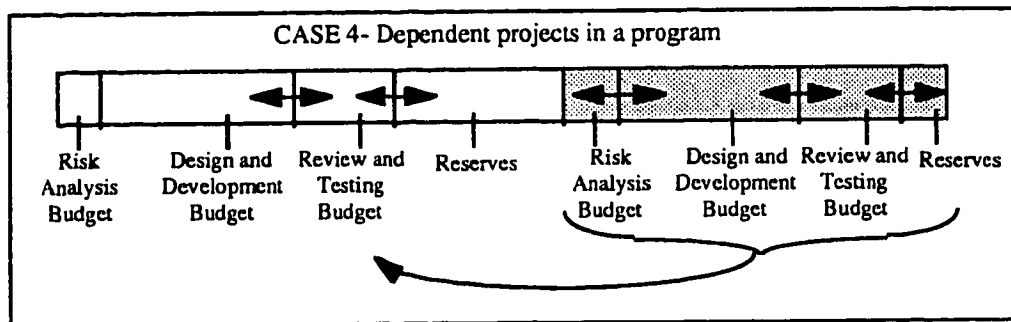


Figure 6.1- Case 4: Management Decisions for Dependent Projects in a Program

The three steps of the PPRM model described in previous chapters are still applicable but must be applied to both of the projects in the program. Specifically, the process is to:

- Optimize project 2 conditional on the possible failure states of project 1, and
- Optimize project 1 with additional penalty costs that reflect the additional costs incurred by project 2 in the case of project 1 failure.

Examples of additional penalty costs to project 1 may include: (1) the costs that project 2 incurs if project 1 fails to develop a new technology component, (2) the costs that project 2 incurs if project 1 fails, and project 2 must redesign a dependent (e.g., communications) subsystem, and (3) the costs of failure of project 2 if it is canceled because of the failure of project 1.

The outputs of the PPRM model for Case 4 are (1) the recommended functional design configuration and components for projects 1 and 2, and (2) the development budget and corresponding reserve budget for each project. Section 6.2 describes the revisions to the PPRM model for examining programs of projects, and Section 6.3 provides an illustration of the program model.

6.2 Program Model Description

The following is a summary of the three steps in the PPRM model described in previous chapters:

STEP 1: Develop and optimize all feasible technical design alternatives over the range of potential project development budgets to minimize each alternative's probability of technical failure.

STEP 2: For each technical design alternative, optimize the strategy to reduce management risks over the range of potential reserve budgets, where the strategy is determined by:

- the potential management problems that could occur for each technical design alternative, and
- potential mitigation actions for each management problem.

STEP 3: Determine the optimal technical design alternative and budget reserve based on the lowest overall expected failure cost given the optimal management risk strategies for that design.

First, the three sequential optimization steps are applied to project 2 conditional on the possible failure states of project 1. The PPRM model quantifies the impact on project 2 of a project 1 failure. Then, the three sequential optimization steps are applied to project 1 with the project 2 penalty costs added to the cost of each failure state for project 1.

6.3 Illustration of PPRM Model for a Program of Two Projects

Consider project 2 first. Assume for example, that project 2 is a small lander mission with a budget of \$120 million (including the launch vehicle) and a schedule duration of 3 years. The lander has one toxicology instrument to check the surface for potential human hazards. With only one instrument, we assume that no partial technical failure states exist. Also, assume that a "perfect" warning system is available for \$1 million and is desired for project 2.

STEP 1: Optimize technical design alternatives.

Step 1.1 Identify the spacecraft functions given the scope of the mission.

The spacecraft functional block diagram is shown in Figure 6.2.

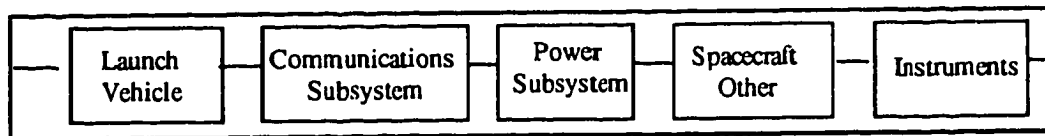


Figure 6.2- Case 4: Project 2 Spacecraft Functional Block Diagram

Step 1.2 Identify the set of functional configurations. Define this set $FIG = \{FIG_1, \dots, FIG_n, \dots\}$.

Two functional configurations are considered. Figure 6.3 shows configuration 1, a single-string design, and Figure 6.4 shows configuration 2, involving a redundant power subsystem.

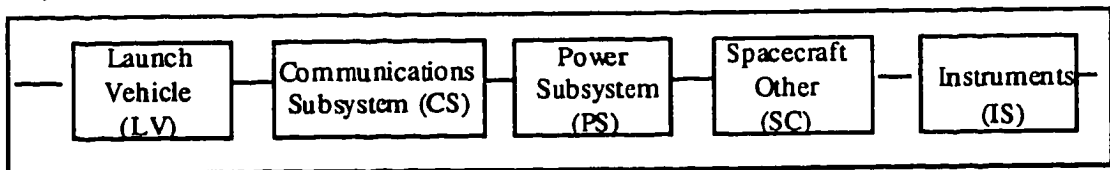


Figure 6.3- Case 4: Project 2, Single-string design, $z = 1$

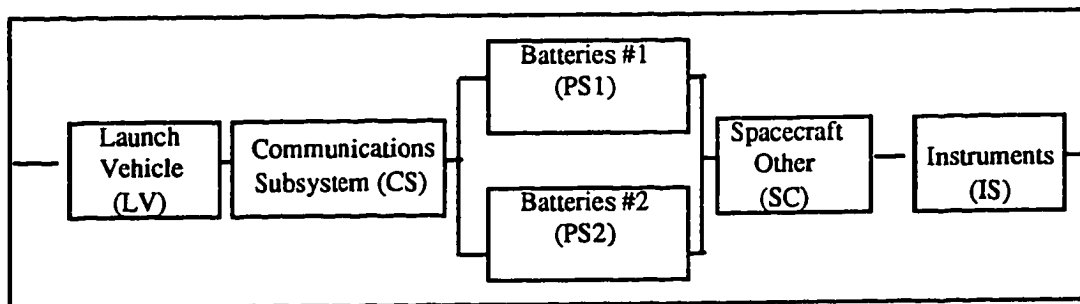


Figure 6.4- Case 4: Project 2, Spacecraft with Redundant Communications System, $z = 2$

Step 1.3 Define AFIG as the set of functional configurations and associated components.
 $AFIG = \{AFIG_{1,1} \dots AFIG_{z,w}, \dots\}$

Step 1.4 For each functional configuration, determine $AFIG_{z,min}$ the lowest-cost alternative.
 Assume $Cost(AFIG_{1,min}) = \$100$ million
 $Cost(AFIG_{2,min}) = \$105$ million

Step 1.5 Fix the risk analysis budget and the schedule allocation.
 The risk analysis budget for project 2 is assumed to be \$0 because the risk analysis of project 2 is performed as part of the project 1 analysis. Development schedule is 34 months with 2 months of schedule reserves.

Step 1.6 Determine the feasible subset of $\{AFIG_{z,min}\}$.
 Both configuration 1 and configuration 2 are feasible.

Step 1.7 For each feasible functional configuration, vary the amount allocated to development and compute the resulting budget surplus as follows:

$$\begin{aligned} \text{Budget surplus} = & \text{Portion of Budget Allocated to Design} - & (6.1) \\ & \text{Cost of Risk Analysis} - \text{Cost}(AFIG_{z,min}) - \text{Cost of Warning System} \end{aligned}$$

\$0 < Budget surplus for configuration 1 < \$19 million
 \$0 < Budget surplus for configuration 2 < \$14 million

Step 1.8 Use a PRA model of the configuration and the Karush-Kuhn-Tucker algorithm to optimize the design based on the cost of improvements, the budget surplus, and associated contributions to the reduction of technical risk : $p(TF|AFIG_{z,w})$.

Configuration 1 (single-string) for project 2

Table 6.1 shows the probabilities of the failure modes for the subsystems in $AFIG_{1,min}$, assuming that all basic event failures are independent.

Table 6.1- Case 4: Probability of Failure Modes, Project 2, Configuration 1

Subsystem	$p(FM_s AFIG_{1,min})$
Launch Vehicle	0.1
Communications Subsystem	0.05
Spacecraft	0.1
Instruments Package	0.05

The probability of technical failure for the lowest-cost design for project 2, configuration 1 is:

$$p(TF | AFIG_{1,min}, WS_1) = \sum_{s \in \{LV, CS, PS, SC, IS\}} p(FM_s | AFIG_{1,min}, WS_1) - \text{"doubles"} + \dots \quad (6.2)$$

$$= 0.279$$

Repeating the optimization process of previous cases, we consider possible reductions of the probability of technical failure given investments in improvements above the minimum or cheapest components, using the data provided in Table 6.2. Figure 6.5 shows on one y-axis, the optimal investment in each subsystem for various levels of investment, and on the second y-axis, the effect of various levels of investment on the probability of technical failure for the system.

Table 6.2- Case 4: Effects of Investment on Reinforcement of Project 2, Configuration 1

Subsystem/ Component	Investment	Reduction Factor
Launch Vehicle	n.a.	n.a.
Communications Subsystem	\$12M	10
Power Subsystem	\$5 M	10
Spacecraft	\$10M	10
Instruments Package	\$10M	10

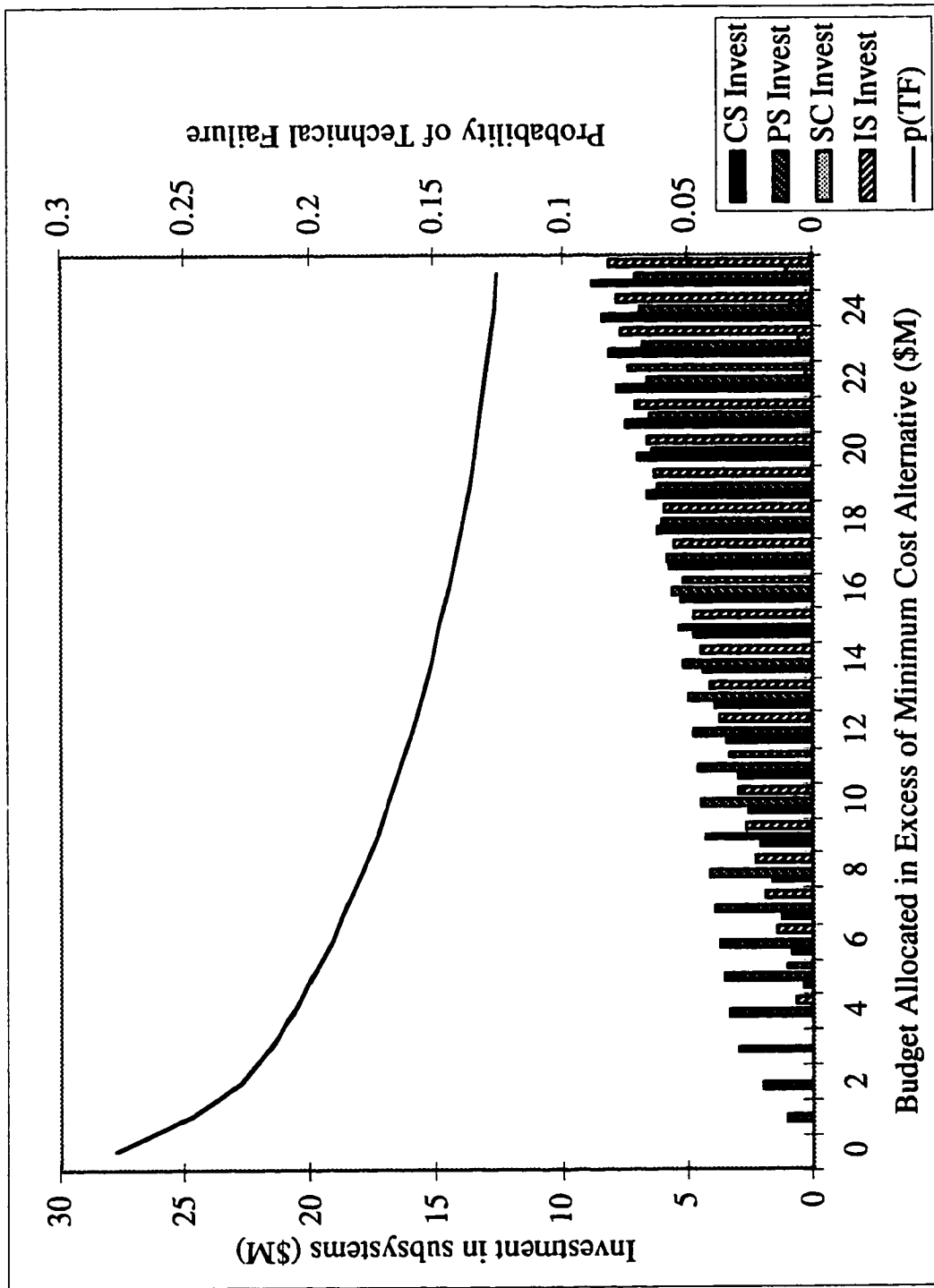


Figure 6.5- Case 4: Various Investment Levels for Project 2, Configuration 1

Configuration 2 (redundant power subsystem) for project 2

Table 6.3 shows the probabilities of the failure modes for the subsystems in $AFIG_{2,min}$, assuming that all basic event failures are independent.

Table 6.3- Case 4: Probability of Failure Modes, Project 2, Configuration 2

Subsystem/ Component	Subsystem Failure $p(FM_i AFIG_{2,min})$
Launch Vehicle	0.1
Communications Subsystem	0.05
Power Subsystem	$p(F_{PS1} AFIG_{2,min}) \times$ $p(F_{PS2} F_{PS1}, AFIG_{2,min}) =$ $0.1 \times 0.1 = 0.01$
Spacecraft	0.01
Instruments Package	0.05

Repeating the optimization process for project 2, configuration 2, we consider possible reductions of the probability of technical failure given investments in improvements above the minimum or cheapest components, using the data provided in Table 6.4. Figure 6.6 shows on one y-axis, the optimal investment in each subsystem for various levels of investment, and on the second y-axis, the effect of various levels of investment on the probability of technical failure for the system.

Table 6.4- Case 4: Effects of Investment on Reinforcement of Project 2, Configuration 2

Subsystem/ Component	Investment	Reduction Factor
Launch Vehicle	n.a.	n.a.
Communications Subsystem	\$12M	10
Power Component 1	\$5 M	10
Power Component 2	\$5 M	10
Spacecraft	\$10M	10
Instruments Package	\$10M	10

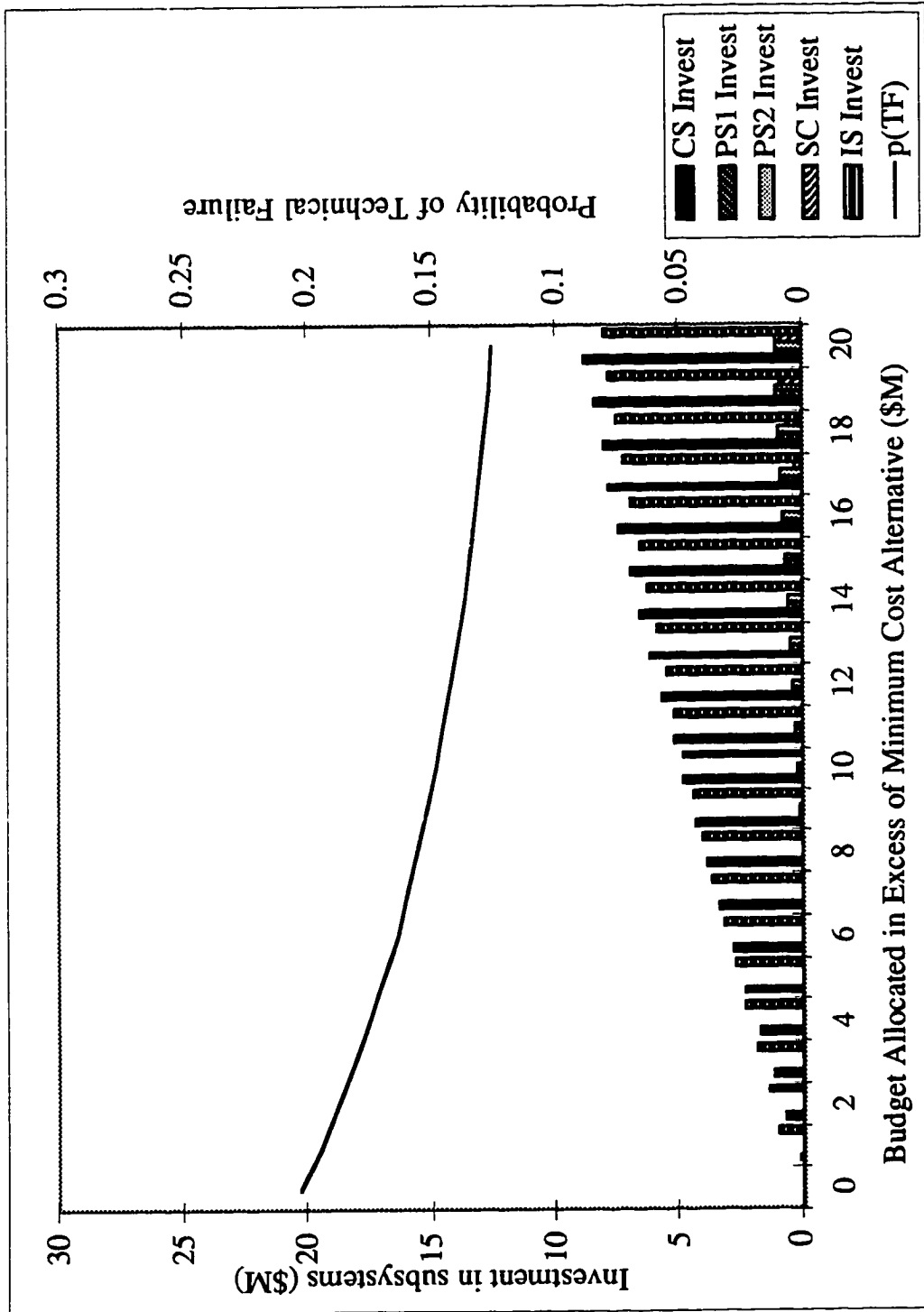


Figure 6.6- Case 4: Various Investment Levels for Project 2, Configuration 2

STEP 2: Optimize the strategy to reduce management risks, conditional on the possible failure states of project 1.

Step 2.1 For each technical design alternative, construct development problem scenarios and possible risk mitigation responses.

Assume that aside from the additional cost of the redundant power system, there are no foreseeable additional management problems. Also, because of the design, there are no potential “descopes” or partial management failures. Table 6.5 shows the potential problems and risk mitigation alternatives for project 2 assuming no failure in project 1.

Table 6.5- Case 4: Management Risk Data for Project 2 (Assuming No Failure in Project 1)

Potential Problems (Risks) conditional on technical design	Probability	Mitigation Alternative 1 (Solve only with \$)	Mitigation Alternative 2		Other Mitigation Alternatives
			(Cost Component)	(Schedule Component)	
components failure thermal test	0.3	\$5 M	\$3 M	1 mo.	n.a.
inadequate spares available	0.6	\$5 M	\$3 M	1 mo.	n.a.
electrical interface problems	0.7	\$3 M	\$2 M	0.5 mo.	n.a.
insufficient assembly/test personnel	0.5	\$3 M	\$1.5 M	1 mo.	n.a.
unknowns	0.5	\$5 M	\$3 M	1 mo.	n.a.

Step 2.2 Resolve the decision tree to determine the probability of each scenario ℓ .

Completed by decision tree resolution (using Precision Tree software) [Palisade Corporation, 1997].

Step 2.3 Determine the outcome for each scenario, conditional on the optimal sequence of risk management options.

Completed by decision tree resolution (using Precision Tree software) [Palisade Corporation, 1997].

Step 2.4 For each design alternative, determine the probability of management failure given the corresponding reserves and the optimal mitigation strategy determined above.

Assuming no failures in project 1, Figure 6.7 shows the probability of management failure for project 2 as a function of the project 2 reserve allocation.

Steps 2.1 through 2.4 are repeated conditional on the various failure states of project 1.
Assume:

- (1) if project 1 descopes the development of the camera technology (PMF), project 2 must spend \$5 million of its reserves on the technology,
- (2) if the camera of project 1 fails (PTF1), project 2 must spend \$6 million of its reserves on additional analysis to select the landing site,
- (3) if project 1 fails completely (either TF or MF) then project 2 must spend an additional \$10 million of its reserves on a different transmitter to relay data (assuming that both components are equally reliable).

For each of these failure scenarios, the probability of management failure is determined as a function of the available reserves as shown in Figure 6.7. For example, since a partial management failure of project 1 requires \$5 million in reserves from project 2, the management failure of project 2 if its reserves are less than \$5 million is certain. As the reserves of project 2 increase beyond the minimum required to resolve the problem resulting from the failure of project 1, the probability of management failure decreases.

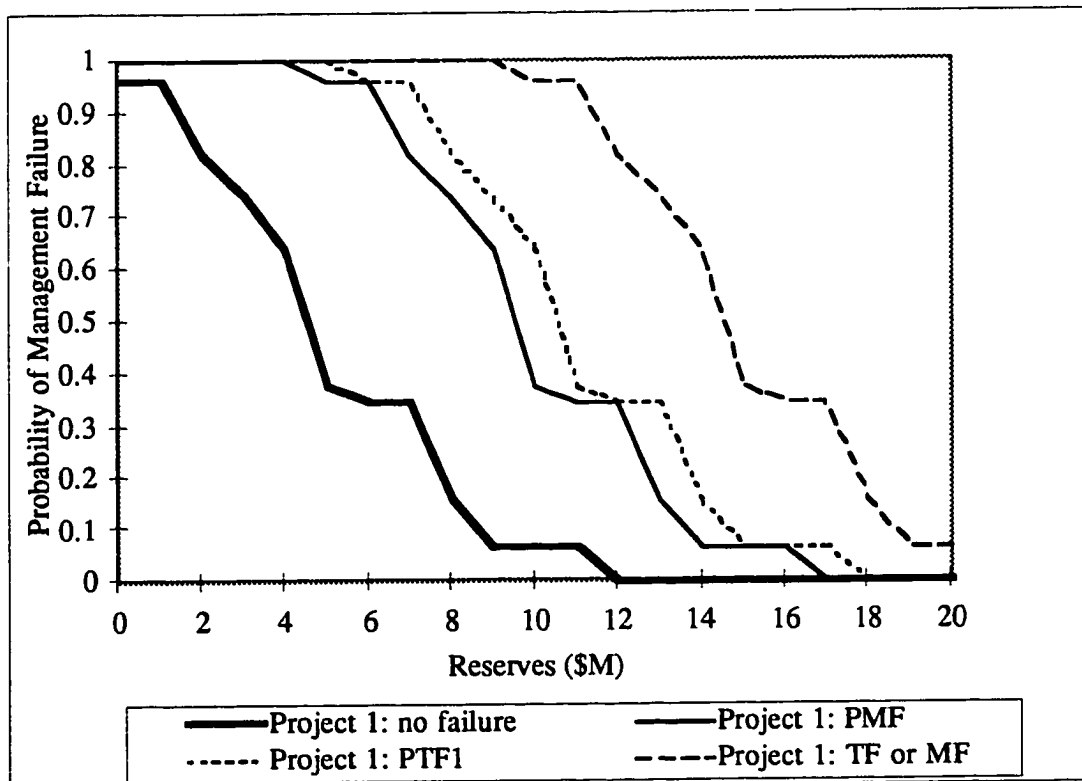


Figure 6.7- Case 4: Probability of Management Failure for Project 2 as a Function of the Reserve Allocation and the Failure Scenario of Project 1

STEP 3: Determine the optimal technical design alternative based on the lowest overall expected failure cost.

Step 3.1 For each alternative, $AFIG_{z,w}$, and the corresponding remaining budget reserve, compute the overall expected failure cost:

$$E(AFIG_{z,w}) = C(MF) \times p(MF|AFIG_{z,w}) + C(TF) \times p(TF|AFIG_{z,w}). \quad (6.3)$$

Assume that the Cost(TF) is \$120, and that the Cost(MF) is \$120

Step 3.2 Determine the optimal technical design alternative.

The optimal design and reserve management strategy for project 2 is conditional on the outcome of Project 1. Table 6.6 shows the optimal technical design alternative conditional on the outcome of Project 1. The cost penalty is the difference between the expected cost of failure of project 2 conditional on the outcome state of project 1.

Table 6.6- Case 4: Optimal Technical Design Alternatives for Project 2 Conditional on the Outcome State of Project 1

	Config.	Develop. (M)	p(TF)	Reserves (M)	p(MF)	E(Cost of Failure) (\$M)	Penalty
No Failure-Project 1	1	\$107	0.19	\$12	0.000	22.8	---
	2	\$107	0.19	\$12	0.000	22.8	
PMF-Project 1	1	\$105	0.20	\$14	0.063	30.0	\$7 M
	2	\$105	0.20	\$14	0.063	30.0	
PTF1-Project 1	1	\$104	0.21	\$15	0.063	31.2	\$8 M
	2	\$105	0.20	\$14	0.153	39.0	
TF/MF-Project 1	1	\$100	0.28	\$19	0.063	39.0	\$16 M
	2	\$105	0.20	\$14	0.639	85.5	

Project 1 with Penalties

Consider now the management of project 1 with the additional penalties associated with the potential effects of project 1 on the performance of project 2.

STEP 1: Optimize technical design alternatives.

Assume unchanged from Case 3.

STEP 2: Optimize the strategy to reduce management risks.

Assume unchanged from Case 3.

STEP 3: Determine the optimal technical design alternative for project 1 based on the lowest overall expected failure cost.

3.1 For each alternative, $AFIG_{z,w}$, and the corresponding remaining budget reserve, compute the overall expected failure cost including the additional penalties from project 2 for failure in project 1.

Assume the following costs of failure:

- $C(TF) = \$166 \text{ M } (\$150 \text{ M } + \$16 \text{ M})$
- $C(MF) = \$166 \text{ M } (\$150 \text{ M } + \$16 \text{ M})$
- $C(PMF) = \$97 \text{ M } (\$90 \text{ M } + \$7 \text{ M})$
- $C(PTF1) = \$98 \text{ M } (\$90 \text{ M } + \$8 \text{ M})$
- $C(PTF2) = \$30 \text{ M}$
- $C(PMF,PTF1) = \$105 \text{ M } (\$90 \text{ M } + \$15 \text{ M})$
- $C(PMF,PTF2) = \$97 \text{ M } (\$90 \text{ M } + \$7 \text{ M})$

Table 6.7 shows the results of optimal design choices for configuration 1. The best technical design alternative for configuration 1 (i.e., the lowest achievable expected cost of failure) is obtained by spending \$133 million on development and keeping \$15 million in reserves. Table 6.8 shows results of optimal the design choices for configuration 2. The best technical design alternative for configuration 2 is obtained by spending \$134 million on development and keeping \$14 million in reserves. The development costs in both tables include \$1 million for the project(s) risk analysis.

Table 6.7- Case 4: Design Alternatives for Project 1, Configuration 1, WS_1 with Additional Program Penalties
(Total Available Budget = \$148M + \$2M for WS_1)

Development (M)	p(TF)	p(PTF1)	p(PTF2)	Reserves (M)	p(MF)	p(PMF)	E(Cost of Failure) (\$M)
\$138	0.152	0.042	0.141	\$10	0.120	0.044	52.1
\$137	0.155	0.045	0.151	\$11	0.094	0.030	48.4
\$136	0.159	0.047	0.161	\$12	0.038	0.016	41.0
\$135	0.164	0.050	0.173	\$13	0.038	0.016	42.1
\$134	0.169	0.053	0.184	\$14	0.019	0.015	40.7
\$133	0.174	0.056	0.197	\$15	0.010	0.006	40.1
\$132	0.180	0.059	0.210	\$16	0.010	0.006	41.5
\$131	0.186	0.062	0.225	\$17	0.002	0.003	41.8
\$130	0.193	0.065	0.240	\$18	0.001	0.002	43.3

Table 6.8- Case 4: Design Alternatives for Project 1, Configuration 2, WS₁ with Additional Program Penalties
(Total Available Budget = \$148M + \$2M for WS₁)

Development (M)	p(TF)	p(PTF1)	p(PTF2)	Reserves (M)	p(MF)	p(PMF)	E(Cost of Failure)
\$140	0.122	0.036	0.117	\$8	0.424	0.037	87.7
\$139	0.123	0.040	0.131	\$9	0.236	0.044	63.3
\$138	0.125	0.043	0.146	\$10	0.236	0.044	64.0
\$137	0.127	0.048	0.163	\$11	0.164	0.052	56.0
\$136	0.129	0.052	0.182	\$12	0.128	0.022	49.8
\$135	0.132	0.057	0.202	\$13	0.128	0.022	51.0
\$134	0.135	0.062	0.224	\$14	0.043	0.024	41.5
\$133	0.140	0.066	0.249	\$15	0.041	0.017	42.3
\$132	0.146	0.068	0.284	\$16	0.032	0.019	43.1
\$131	0.153	0.060	0.357	\$17	0.015	0.006	41.9

The recommendation is to choose the single-string configuration, spend \$133 million in development (\$2.8 million in the communications system, \$1.5 in instrument 1 (camera), and \$3.7 million in instrument 2), and retain \$15 million in reserves to mitigate potential problems. The expected cost of failure of the optimal alternative increases from \$36.8 million to \$40.1 million when the potential failure effects of project 2 are included (Table 5.5 and Table 6.7).

What if a technical failure of project 1 is discovered too late to change project 2, and therefore if project 1 experienced a technical failure such that project 2 would also be considered a failure?

Assume the following costs of failure:

- $C(TF) = \$270 \text{ M } (\$150 \text{ M } + \$120 \text{ M})$
- $C(MF) = \$166 \text{ M } (\$150 \text{ M } + \$16 \text{ M})$
- $C(PMF) = \$97 \text{ M } (\$90 \text{ M } + \$7 \text{ M})$
- $C(PTF1) = \$98 \text{ M } (\$90 \text{ M } + \$8 \text{ M})$
- $C(PTF2) = \$30 \text{ M}$
- $C(PMF,PTF1) = \$105 \text{ M } (\$90 \text{ M } + \$15 \text{ M})$
- $C(PMF,PTF2) = \$97 \text{ M } (\$90 \text{ M } + \$7 \text{ M})$

Table 6.9 shows the results of optimal design choices for configuration 1. The best technical design alternative for configuration 1 (i.e., the lowest achievable expected cost of

failure) is obtained by spending \$134 million on development and keeping \$14 million in reserves. Table 6.10 shows the results of optimal design choices for configuration 2. The best technical design alternative for configuration 2 is obtained by spending \$134 million on development and keeping \$14 million in reserves. The development costs in both tables include \$1 million for the project(s) risk analysis.

Table 6.9- Design Alternatives for Project 1, Configuration 1, WS₁ with Large Program Penalties for Technical Failure
(Total Available Budget = \$148M + \$2M for WS₁)

Development (M)	p(TF)	p(PTF1)	p(PTF2)	Reserves (M)	p(MF)	p(PMF)	E(Cost of Failure) (\$M)
\$138	0.152	0.042	0.141	\$10	0.120	0.044	65.9
\$137	0.155	0.045	0.151	\$11	0.094	0.030	63.0
\$136	0.159	0.047	0.161	\$12	0.038	0.016	56.9
\$135	0.164	0.050	0.173	\$13	0.038	0.016	58.5
\$134	0.169	0.053	0.184	\$14	0.019	0.015	57.9
\$133	0.174	0.056	0.197	\$15	0.010	0.006	58.0
\$132	0.180	0.059	0.210	\$16	0.010	0.006	60.0
\$131	0.186	0.062	0.225	\$17	0.002	0.003	61.1
\$130	0.193	0.065	0.240	\$18	0.001	0.002	63.3

Table 6.10- Design Alternatives for Project 1, Configuration 2, WS₁ with Large Program Penalties for Technical Failure
(Total Available Budget = \$148M + \$2M for WS₁)

Development (M)	p(TF)	p(PTF1)	p(PTF2)	Reserves (M)	p(MF)	p(PMF)	E(Cost of Failure) (\$M)
\$140	0.122	0.036	0.117	\$8	0.424	0.037	95.0
\$139	0.123	0.040	0.131	\$9	0.236	0.044	73.1
\$138	0.125	0.043	0.146	\$10	0.236	0.044	73.9
\$137	0.127	0.048	0.163	\$11	0.164	0.052	67.0
\$136	0.129	0.052	0.182	\$12	0.128	0.022	61.5
\$135	0.132	0.057	0.202	\$13	0.128	0.022	62.9
\$134	0.135	0.062	0.224	\$14	0.043	0.024	54.9
\$133	0.140	0.066	0.249	\$15	0.041	0.017	56.2
\$132	0.146	0.068	0.284	\$16	0.032	0.019	57.7
\$131	0.153	0.060	0.357	\$17	0.015	0.006	57.6

The recommendation is to choose the partially redundant configuration, spend \$134 million in development and retain \$14 million in reserves to mitigate potential problems. The expected cost of failure of the optimal alternative for project 1 increases from \$36.8 million to \$54.9 million when the potential failure effects on project 2 are included.

With the large penalty costs assigned to a technical failure of project 1, the preferred alternative shifts from configuration 1 to configuration 2. Configuration 2 is preferred because for the equivalent \$134 million development budget, the probability of technical failure is lower in the partially redundant system. Therefore, here, considering the effects of failures of project 1 on project 2 does affect the management of project 1.

6.4 Summary for Case 4

Case 4 extended the PPRM model to quantify the dependencies among projects in a program. The dependencies are represented by a penalty cost added to the cost of failure of the first project. This penalty cost is the amount of additional costs that a future project can incur because of the failure of the first project. As was shown in the illustration, the dependencies among projects and the associated magnitude of possible penalty costs can influence the preferred technical design alternative for the initial project (project 1) because it can affect the performance of project 2.

CHAPTER 7

Recommendations, Conclusions and Future Research

7.1 Research Summary

In order to structure and manage programs of interdependent projects effectively, managers must: 1) divide the resources into project budgets and reserves, 2) manage the project resources to maximize technical reliability, and 3) manage the reserves to minimize management failures while considering the dependencies among projects. In the absence of a formal means for quantifying and modeling potential risk tradeoffs, decision makers may not optimally allocate the resources available. This research provides a mathematical framework for addressing this problem.

The PPRM model is a sequence of three optimization steps. The first step develops and optimizes feasible technical design alternatives over the range of potential budgets to minimize each alternative's probability of technical failure. The second step identifies potential management risks associated with each alternative and optimizes the risk mitigation strategy as a function of the budget reserve. The third step determines the optimal technical design alternative and the budget reserve based on the lowest overall failure cost considering both technical and management failure.

The PPRM model was presented and illustrated for a series of cases. First, the model identified, for one project, the optimal design configuration, choice of components, and budget reserves. The illustration of this case demonstrated that even for tightly constrained projects, single-string systems are not always better. Specifically, if significant investment is required to make a single-string design sufficiently reliable, a partially redundant system may be preferable.

Second, the model considered the same decisions in conjunction with the optimal level of testing and reviews ("warning systems"). The illustration of this case showed that investment in a reliable warning system is important if significant failure risks exist from undetected problems in the system. There is a point, however, when the costs of a more reliable warning system are too large, and the money could be better spent reinforcing the system or solving management problems.

Third, the model considered the same decisions for one project, but also included the possibility of partial failures. An important input to the illustration for this case was how much of a “failure” was a partial failure in the managers' opinion. The illustration demonstrated that if the cost impact of the partial failure states was significant, the preferred alternative could change as budget resources are shifted to development in order to further reinforce the design against partial failures.

Finally, the model examined the management of one project when the outcome of that project can affect the performance of other projects in the program. The illustration of this case showed that the magnitude of the dependencies among the projects can influence the preferred technical design alternative for the first project.

The primary contribution of this research is the development of a decision support model to analyze interdependent projects within programs, explicitly including the probabilities and consequences of technical and management failures. The model is intended to improve both the design process for the physical system and the management of the resource reserves to maximize the decision maker's expected utility for the outcome(s) of a whole program. While the utility function used in the illustrations approximates the decision maker's preferences for mission outcomes by the expected costs of failure of the mission, any utility function that includes both managerial and technical success can be incorporated in the model.

The illustrations in this dissertation focused on space missions, however, the PPRM model has much broader applicability. Important characteristics of potential areas of application include projects developed with tightly constrained resources and dependencies among projects in a program. An interesting field may be the semiconductor industry where the development schedules are fast and the dependencies between the next chip design and the previous one are large.

The model and illustrations presented in this dissertation were implemented with two commercial software packages: Palisade Corporation's Precision Tree and Microsoft's Excel. Precision Tree is a decision analysis software package that is an “add-in” to Microsoft's Excel. The Excel solver tool was used to optimize the investments in the technical design. Precision Tree was used to solve the decision trees required to determine the optimal risk mitigation strategy, and Excel was used to quantify the lowest achievable expected cost of failure for each alternative. In order to implement this model in a real

situation, additional probabilistic risk analysis modeling tools may be necessary to quantify the functional relationship between investment in the components and subsystems and the probability of technical failure for the system.

In [Madden, 1996], one of the lessons learned from previous NASA projects is that: “The seeds of problems are laid down early. Initial planning is the most vital part of a project. The review of most failed projects or project problems indicate the disasters were well planned to happen from the start.” Using the forward-looking PPRM model can help project managers to follow a systematic approach, considering in the planning phase of a program all risks, alternatives and interactions among projects, thus anticipating and hopefully preventing possible failures.

7.2 Conclusions and Recommendations for Structuring and Managing Programs of Projects

In conclusion, the PPRM model developed in this dissertation provides the decision maker with a formal approach to implement each of the following recommendations.

Consider the value of the risk analysis before investing considerable resources.

The PPRM model as described in this dissertation requires a technical probabilistic risk analysis (PRA) model and additional analysis of the potential management risks. This detailed analysis may be helpful if the problem is complex, if the risks involve potentially high consequences, or if the public is particularly sensitive to the situation (e.g., problems involving nuclear fuel). This analysis has positive value if the resulting improvements to the design of the system when compared to an experience-based design, reduce the expected cost of mission failure by more than the cost of the analysis. Clearly, in resource-constrained projects, time and money should be spent only on analyses that have positive value.

Don't plan and manage dependent projects independently. The most important reason for modeling a program is to analyze the potential dependencies among the projects. Understanding which risks have the greatest impact on other projects represents important information in the decision making process. Resource allocation and risk mitigation decisions for each project should be made to minimize both the technical and management risks for all projects in a program.

Don't set arbitrary constraints without careful consideration of their effects on the performance of the project and the whole program. An additional \$1 million on a \$200 million project may add significant benefit to the value of the mission or the reduction of risks. Decision makers can use the PPRM model to examine the shadow "risk cost" associated with the budget constraint, and develop supportive evidence to justify any requests for increases in the project resources.

Adjust the scope of the project to the budget and schedule constraints. Determine the optimal size of the project based on the resources, avoid project requirements "creep," and don't change the scope midstream. Determine the optimal scope based on a trade-off between the value of the mission and the level of project risk given the available resources. Empirical analysis of past project show that adding scope and requirements after the design and resource allocation have been optimized can significantly increase the probability of project failure, in particular, management failure.

Reserves should be established based on careful consideration of all uncertainties. The quantity of budget held in reserves is the primary factor in mitigating management risks. Money held in reserves, however, is money that is not spent to design the system or increase its reliability. Project managers should choose the optimal technical design alternative to minimize the expected cost of failure (both technical and managerial) for the project, and the amount of resources to allocate to budget reserves is an output of this analysis.

Evaluate the decision to develop new technologies on a project considering the increase of management risks involved. Don't develop new technologies within projects unless: (1) there is some flexibility in resources, (2) the technology is mature enough so that the uncertainties are acceptable, and (3) the timing of the funding and the level of reserves reflect the uncertainty remaining in the development process. The PPRM model is useful in modeling the management risks associated with new technology development within a project, with the outcome of failed research and development defined as a partial management failure.

7.3 Limitations and Future Research Directions

While the framework presented in this dissertation is an important step in providing decision support for managing programs of interdependent projects, it has clear limitations in its current form.

Optimal allocation of schedule

In this dissertation, the focus was the optimal allocation of budget between the project development and the reserves. The schedule reserve was considered a factor in the probability of management failure, but the schedule allocation was not. Instead, the trade-off between schedule and budget was accounted for on a case-by-case basis in the identification of risk mitigation scenarios and the minimization of the probability of management failure. This trade-off was based on a fixed schedule reserve. In order to include the allocation of schedule in the PPRM model, the relationship between the probability of technical failure and the development schedule needs to be defined. In future work, the optimization of the technical design should depend on the schedule allocated to development.

Allocation of resources among projects in a program

In this dissertation, we focused primarily on one project and examined how potential project outcomes could affect other projects in a program. Future work should include the capability to reallocate resources among projects in a program, similar to the shifting of resources in a single project between development and reserves. This reallocation process should rely on the shadow cost of the constraints to determine the optimal decision.

Reliance on expert opinion and use of previous test results

One unavoidable problem in the implementation of the PPRM model is that one often lacks applicable statistical data that describe the project or program. Because the model relies on the use of a PRA at an early stage in the system design, it is important to have access to previous test data that can provide probabilities in that phase. Often, however, relevant test data about potential problems and failure modes are not available. Data collection and elicitation of expert opinions often proves to be the most time-consuming parts of the analysis. Research is currently performed in the field of risk analysis to improve the use of expert assessment in risk models [Keeney and von Winterfeldt, 1991, Hora and Iman, 1989, and USNRC, 1987]. It is also important to improve the storage and retrieval of any applicable data such as previous test results.

This dissertation describes an approach for quantifying both technical and managerial risks in interdependent projects within a program. By following such an approach, managers can balance the tradeoffs between these risks. In the past, effective program management has indeed been displayed for complex technical systems. The type of analytical tools described here, however, can be a useful complement to experience and intuition. These techniques can enable managers to explicitly examine tradeoff decisions critical to project success.

REFERENCES

- Archibald, R.: *Managing High-Technology Programs and Projects*. New York: John Wiley and Sons, 1992.
- Bradley, R.M., M.G. Powell, and M.R. Soulsby: Quantifying Variations in Project-Cost Estimates. *Journal of Management in Engineering* 6:99-106 (1990).
- Bubushait, K.A.: A Survey of the Practices of Project Management Techniques in Different Industries. In *Project Management Institute Seminar/Symposium, Montreal, Canada, Sept. 20-25, 1986*. pp. 132-138.
- Burke, C.M. and S.C. Ward.: Project appraisal- finance approaches to risk. In *Developments in Operational Research*. N.B. Cook and A.M. Johnson (eds.), 1988.
- Chapman, C.B. and S.C. Ward.: *Project Risk Management: Processes, Techniques, and Insights*, Chicester: John Wiley and Sons, 1997.
- Cleland, D.I.: *Project Management: Strategic Design and Implementation, 2nd edition*. New York: McGraw-Hill, Inc., 1994.
- Cooper, D.F. and C.B. Chapman: *Risk Analysis for Large Projects*. New York: John Wiley and Sons, 1987.
- Covello, V.T.: Decision Analysis and Risk Management Decision Making: Issues and Methods. *Risk Analysis* 7:131-139 (1987).
- Eisner, H.: *Essentials of Project and Systems Engineering Management*. New York: John Wiley and Sons, 1997.
- Fragola, J., R. Kurth, G. Maggio, S. Epstein, and M. Frank: Probabilistic Risk Analysis Applied to the Space-Shuttle Main Engine. In *1994 Proceedings of the Annual Reliability and Maintainability Symposium*, 1994. pp. 494-503.
- Garrick, J.B.: Recent Case Studies and Advancements in Probabilistic Risk Assessment. *Risk Analysis* 4:267-279 (1984).
- Henley, E. and H. Kumamoto: *Probabilistic Risk Assessment: Reliability Engineering, Design, and Analysis*. New York: IEEE Press, 1992.
- Hertz, D.B.: Risk analysis in capital investment. *Harvard Business Review* 42:95-106 (1964).
- Hillier, F.S. and G.J. Lieberman: *Introduction to Operations Research*. New York: McGraw-Hill, 1990.
- Hora, S.C., and Iman, R.L.: Expert opinion in risk analysis: The NUREG 1150 methodology. *Nuclear Science and Engineering* 102:323-331 (1989).

- Howard, R.A: Information Value Theory. In *The Principles and Applications of Decision Analysis*. R.A. Howard and J.E. Matheson (eds.), Palo Alto, CA: Strategic Decisions Group, 1989.
- Hulett, D.: Project Schedule Risk Assessment. *Project Management Journal* 26:21-31 (1995).
- Jaselskis, E.J. and D.B. Ashley: Optimal Allocation of Project Management Resources for Achieving Success. *Journal of Construction Engineering and Management* 117:321-340 (1991).
- Kaplan, S. and B.J. Garrick: On the Quantitative Definition of Risk. *Risk Analysis* 1:11-27 (1981).
- Keeney, R.L.: *Value-Focused Thinking: A Path to Creative Decisionmaking*. Cambridge, Massachusetts: Harvard University Press, 1992.
- Keeney, R.L. and H. Raiffa: *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*. Massachusetts: Cambridge University Press, 1993.
- Keeney, R.L. and D. von Winterfeldt: Eliciting Probabilities from Experts in Complex Technical Problems. *IEEE Transactions on Engineering Management* 38:191-201 (1991).
- Kidd, J.B.: A Comparison Between the VERT Program and Other Methods of Project Duration Estimation. *OMEGA* 15:129-134 (1987).
- Lakats, L.: "Designing Human and Technical Systems for the Communication of Critical Information: A Systems Analysis Approach." Ph.D. diss., IEEM Department, Stanford University, Stanford, CA, 1997.
- Lee, S., G. Moeller, and L. Digman: *Network Analysis for Management Decisions*. Boston: Kluwer-Nijhoff Publishing, 1982.
- Madden, J.: *One Hundred Rules for NASA Project Managers, Lessons Learned*: NASA, 1996.
- Matheson, J.E.: The Economic Value of Analysis and Computation. In *The Principles and Applications of Decision Analysis*. R.A. Howard and J.E. Matheson (eds.), Palo Alto, CA: Strategic Decisions Group, 1989.
- Matheson, J.E., and R.A. Howard: An Introduction to Decision Analysis. In *The Principles and Applications of Decision Analysis*. R.A. Howard and J.E. Matheson (eds.), Palo Alto, CA: Strategic Decisions Group, 1989.
- Moder, J., C. Phillips, and E. Davis: *Project Management with CPM, PERT, and Precedence Diagramming*. New York: Van Nostrand Reinhold Company, 1983.
- Morris, P.W.G.: Research at Oxford into the Preconditions of Success and Failure of Major Projects. In *Project Management Institute Seminar/Symposium, Montreal, Canada, Sept. 20-25, 1986*. pp. 53-66.
- NASA Advisory Council: *Report of the Cost Assessment and Validation Task Force on the International Space Stations*. Washington, D.C.: NASA, 1998.

- NASA Jet Propulsion Laboratory: *Microrover Flight Experiment: Risk Management Progress Report* (JPL D-11181-4). Pasadena, California: Jet Propulsion Laboratory, 1996.
- NASA Jet Propulsion Laboratory: "Mars Pathfinder winds down after phenomenal mission," Press Release, NASA Jet Propulsion Laboratory, Pasadena, CA, November 4, 1997.
- NASA Jet Propulsion Laboratory: "Mars Architecture Workshop Presentation." July 27, 1998a.
- NASA Jet Propulsion Laboratory: "DS2 Web-site" (<http://nmp.jpl.nasa.gov/ds2>). December 1998b.
- NASA Jet Propulsion Laboratory: "MGS Web-site" (<http://mars.jpl.nasa.gov/mgs>). December 1998c.
- Palisade Corporation: *Precision Tree: Decision Analysis Add-In for Microsoft Excel*, Newfield, NY, July 1997.
- Paté-Cornell, M.E.: Warning Systems in Risk Management. *Risk Analysis* 5:223-234 (1986).
- Paté-Cornell, M.E.: Learning from the Piper Alpha Accident: A Postmortem Analysis of Technical and Organizational Factors. *Risk Analysis* 13:215-232 (1993).
- Paté-Cornell, M.E.: Uncertainties in risk analysis: Six levels of treatment. *Reliability Engineering and System Safety* 54:95-111 (1996).
- Paté-Cornell, M.E. and R.L. Dillon: Challenges in the Management of Faster-Better-Cheaper Space Missions. In *Proceedings of IEEE Aerospace Conference*, Snowmass, Colorado, (1998a).
- Paté-Cornell, M.E. and R.L. Dillon: Analytical Tools for the Management of Faster-Better-Cheaper Space Missions. In *Proceedings of IEEE Aerospace Conference*, Snowmass, Colorado, (1998b).
- Pinkus, R.L., L.J. Shuman, N.P. Hummon, and H. Wolfe: *Engineering Ethics: Balancing Cost, Schedule, and Risk- Lessons Learned from the Space Shuttle*. Cambridge: Cambridge University Press, 1997.
- RAND Corporation: *Understanding the Outcomes of Megaprojects: A Quantitative Analysis of Very Large Civilian Projects* by E.W. Merrow (R-3560-PSSP). Santa Monica, CA: The RAND Corporation, March 1988.
- RAND Corporation: *Understanding Cost Growth and Performance Shortfalls in Pioneer Process Plants* by E.W. Merrow, K.E. Phillips, and C.W. Myers (R-2569-DOE). Santa Monica, CA: The RAND Corporation, September 1981.
- RAND Corporation: *A Review of Cost Estimation in New Technologies* by E.W. Merrow, S.W. Chapel, and C. Worthing (R-2381-DOE). Santa Monica, CA: The RAND Corporation, July 1979.

- Reiter, D., M.E. Paté-Cornell, and R.L. Dillon: *An Analytical Approach to Determining the Value of Proposed NASA Missions* in preparation, 1999.
- Ruskin, A.: *What Every Engineer Should Know About Project Management, 2nd edition.* New York: Marcel Dekker, 1994.
- Sapolsky, H.: *The Polaris System Development.* Massachusetts: Harvard University Press, 1972.
- Shirley, D. and D. McCleese: Mars Exploration Program Strategy: 1995-2020. *34th Aerospace Sciences Meeting and Exhibit*, Reno, NV: Jan. 15-18, 1996.
- Shishko, R.: *NASA Systems Engineering Handbook* (NASA SP-6105), June 1995.
- Shtub, A., J. Bard, and S. Globerson: *Project Management: Engineering, Technology, and Implementation.* Englewood Cliffs, NJ: Prentice Hall, 1994.
- Tversky, A. and D. Kahneman: Judgment Under Uncertainty: Heuristics and Biases. *Science* 185:1124-1131 (1974).
- US Nuclear Regulatory Commission: *Reactor Safety Study: Assessment of Accident Risk in U.S. Commercial Nuclear Plants, WASH-1400* (NUREG-75/014). Washington, D.C.: U.S. Nuclear Regulatory Commission, 1975.
- US Nuclear Regulatory Commission: *Nuclear Regulatory Commission, "NUREG 1150, Draft,"* Washington, D.C.: U.S. Nuclear Regulatory Commission, 1987.
- Van Slyke, R.M.: Monte Carlo methods and the PERT problem. *Operations Research* 11:839-860 (1963).
- von Winterfeldt, D. and W. Edwards: *Decision Analysis and Behavioral Research.* Massachusetts: Cambridge University Press, 1986.
- Weist, J.: Gene-splicing PERT and CPM: The Engineering of Project Network Models. *Project Management: Methods and Studies.* Burton Dean (ed.), Amsterdam: North-Holland, 1985, pp. 67-94.
- Williams, T.: A classified bibliography of recent research relating to project risk management. *European Journal of Operational Research* 85:18-38 (1995).
- Williams, T.: Using a risk register to integrate risk management in project definition. *International Journal of Project Management* 12:17-22 (1994).
- Williams, T.: Risk-management infrastructures. *International Journal of Project Management* 11:5-10 (1993).
- Williams, T.: Risk analysis using an embedded CPA package. *International Journal of Project Management* 8:84-88 (1990).