'Risk/Requirements Trade-off Guidelines for Low Cost Satellite Systems

Steven L. Cornford and Kin F. Man

Jet Propulsion Laboratory
California Institute of Technology
4800 Oak Grove Drive
Pasadena, CA 91109

Abstract

The accelerating trend toward Faster, Better, Cheaper (FEE) missions places increasing emphasis on the trade-offs between requirements and risk to reduce cost and development times, while still improving quality and reliability. The Risk/Requirements Trade-off Guidelines discussed in this paper are part of an integrated approach to address the main issues by focusing on the sum of prevention, analysis, control or test (PACT) processes. This approach maps weighted risk (or failure modes) against detection or prevention options to provide a mechanism for performing risk/resource trade-offs. The population of this matrix can be done a "row at a time" by examining the value added of each requirement or PACT, in terms of risk reduction, This row by row development is the principle focus of the guidelines described herein. Cost drivers in the performance of these specific areas are identified for potential trade-off studies. Parametric trade-offs that would be cost effective are indicated and effective substitutes for specific requirements are discussed.

1. Introduction

In the quest to achieve FBC missions, NASA is increasing the use of new technologies in its missions. The use of non-flight qualified technologies may entail a higher level of risk to the missions. The requirements that have been developed over the years tend to be for more conservative missions, when only performance counted and money was not as much of an issue. This philosophy is no longer justifiable in the present environment. Projects are now more concerned with requirements which may drive up cost, increase schedule, affect risk, and introduce uncertainty, l-he effects and consequences of introducing or changing requirements, particularly on the cost and risk, need to be well understood. The risk/requirements trade-off guidelines developed and described in this paper' are intended to help projects understand the relationship between requirements and risk to enable trade-offs to be made in a rational way to reduce cost and development times, while still improving quality and reliability.

2. Project Risk

Risk is inherent in all projects and endeavors. It is defined as the likelihood of a flight element not performing as expected. The level of risk depends on the adverse consequences of a non-conformance of the hardware, as well as programmatic elements such as schedule and cost. In order to manage risk in a project, there needs to be a systematic approach to identifying and assessing the sources of risk to allow decisions and trade-offs to be made. In the current era of best effort for a fixed cost, every resource has to be evaluated on an equal footing and trade-offs made to optimize project success. Taking an increasing amount of risk may be inevitable for future low cost missions, but taking more risk does not necessarily mean a reduction in success rate. This seemingly contradictory statement is a result of the diminishing returns on risk reduction. For example, if one S/C with 0.95 probability of survival cost $250M, but three S/C with 0.8 probability of survival cost $50M each, then one increases the expected value of success (0.95 to 2,4) while lowering cost ($250M to $150M). This concept and implication are discussed further in Reference 1. For low cost missions, risks are to be managed rather than avoided. A risk mitigation approach needs to be implemented right from the beginning to identify and evaluate the risks involved and implement cost-effective mitigation strategies. An approach has been developed [Ref. 2] which identifies "tall poles" and various detection or prevention options and the associated costs. The process for trade-offs between all project elements can be rather complex. Sometimes it may be necessary to take on more risk by integrating more advanced commercial, non-flight qualified technologies to increase capabilities, and reduce cost and schedule. The overall risk of such action has to

be weighed against the acceptable level of risk of the whole mission. For example, the criteria for success of a technology demonstration flight are very different from a science mission. The consequences of these risks have to be identified, understood and led to informed decisions.

3. Project Requirements

Over the past 35 years, NASA's requirements on projects and missions have continued to grow. These requirements include mission; science; environmental; test, analysis and integration; system performance; etc., not to mention the requirements for cost, schedule and risk. Most of these are essential to maximize the success of projects. While some are in response to federal requirements, many are merely the acceptance of procedure which may have outlived whatever usefulness they once had. It is unproductive to tty to impose the proposal, contracting, qualification, and review procedures which were applicable for the "take no risk" paradigm onto projects when NASA is attempting to significantly lower cost by adopting a new spacecraft development philosophy, I-he necessity and value of these requirements must be rc-assessed to ensure the cost of meeting requirements does not exceed the value added of those requirements. Only those with sufficient net value-added should be implemented. Procedures and requirements need to be reviewed from a "zero based" approach where each selection is examined based on its benefit compared with its cost and risk.

Currently there is a NASA-funded effort at JPL to develop a methodology for evaluating the merit of each requirement and the cost of implementation. This "Requirements Reduction" task (see Figure 1) is focusing on product assurance requirements for projects. The goal is to reduce product assurance requirements and the risk to a project by implementing a systematic approach and by allowing resources to be focused on areas with the greatest return.

4. Guideline Objectives

As the trend towards FBC missions accelerates, it presents managers and project personnel with additional challenges of devising streamlined guidelines for implementing this new way of doing business. Thus, there is a renewed emphasis on tradeoffs between requirements and risk to reduce cost and development times, while still improving quality and reliability, The risk/requirements tradeoff guidelines described in this paper are intended to assist projects in this endeavor for the product assurance arena. The objectives of the requirements contained in these guidelines can be summarized generically as: to 1) demonstrate operation in a flight-like environment; 2) validate design; 3) demonstrate robustness; 4) detect workmanship flaws; and 5) demonstrate reliability. Each guideline addresses one or more of these objectives. The definitions of these objectives, as used in the context of this work, are defined below:

1. Demonstrate operation in a flight-like environment — demonstrate hardware operation to design levels in a flight-like environment in which several operational parameters may interact synergistically with each other and with the test environment.
2. Validate design — demonstrate the ability of the electrical and/or mechanical hardware design to function within specifications in various operational modes (on/off cycles, start-up performance, deployment times, end-of-life conditions, etc.) and anticipated environments,
3. Demonstrate robustness – demonstrate the ability of a unit to operate at levels beyond the expected flight/use environment, in order to quantify the various margins within a design, Testing to the limits of performance should not physically break or cause irreversible degradation or damage. Robustness demonstration typically involves electrical, mechanical, and thermal margins (e.g. sensitivity to voltage, clock frequencies, packaging design performance, thermal degradation, structural integrity, etc.),
4. Detect workmanship flaws — detect workmanship flaws that can cause time-dependent degradation to electrical and mechanical hardware, as well as non-time dependent failures, Workmanship flaws can result both from process variations in assembly and integration, and those that escaped from lower-level manufacturing operations,
5. Demonstrate reliability — demonstrate the ability of the flight hardware to operate the required functions under specified conditions for a stated period of time. Sufficient operating time is accumulated through testing

to eliminate “infant-mortality” defects and to provide a measure of the expected failure rate.

5. Guideline Development Approach

Utilizing the results of the Requirements Reduction effort (Figure 1), for each issue identified with its recommended requirement, the influence on the risk of increasing or reducing the requirements are determined, e.g. once a test level and duration are identified the risk circumstance created by parametric variation are identified. A higher test level may allow a shorter test duration and reduce cost, a longer test duration may permit lower test levels, enabling adequate accumulated stress, yet lowering the risk of test failure, A concept of requirements as “black boxes” through which product is passed to emerge with the risk identified or mitigated has been developed. Each of these requirements may then be thought of as having “knobs” or allowable parametric variations. The efficacy and sensitivity of each ‘(knob setting” versus specific risk elements may then be quantified. These are captured within the guidelines and thus provide criteria for elimination or modification of product assurance elements, They provide insight to permit decision makers to understand the issues and the cost, risks, and benefit of changing the requirement.

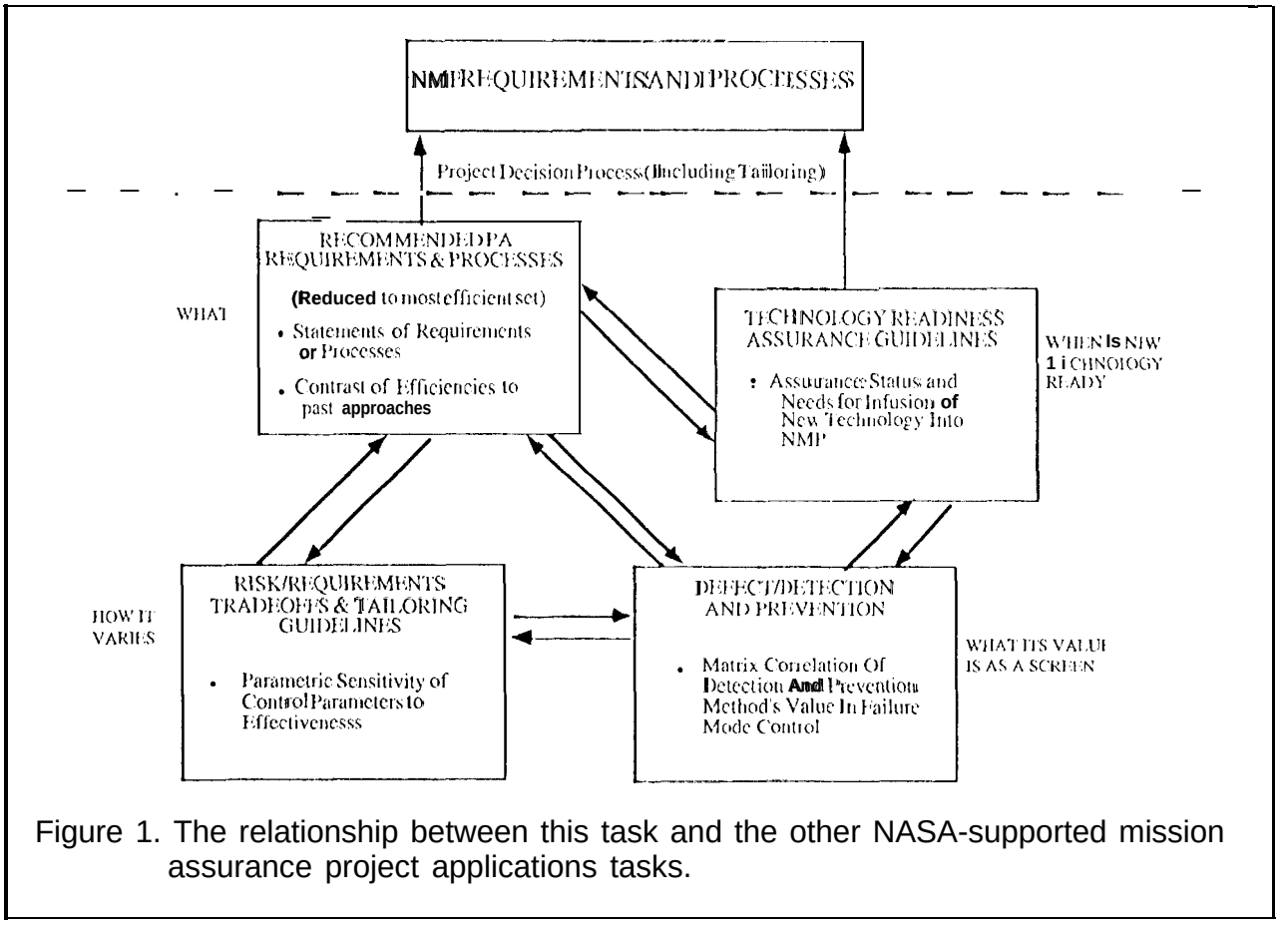

Figure 1. The relationship between this task and the other NASA-supported mission assurance project applications tasks.

These guidelines are the evolving product of the Risk/Requirements Tradeoff task. This task is part of a suite of four tasks in the New Millennium Mission Assurance Project Applications RTOP, sponsored by the Payloads/Aeronautics Division (QT) of the Office of Safety and Mission Assurance (Code Q) at NASA, This suite of tasks (Figure 1) is designed to function synergistically to enable the emerging needs of microspacecraft (p-S/C), in particular the New Millennium Program, and to remove the roadblocks for achieving their goals. The first of the four tasks, the Recommended Product Assurance Requirements and Processes task, determines criteria for a minimum set of product assurance requirements to ensure mission success, It initially recommends a set of specific reliability, environmental, parts, and quality requirements for p-S/C applications. For each of the issues identified in the first task, the second task, in the

fern] of tradeoff and tailoring guidelines described in this paper, determines the impact on the risk of increasing or reducing the "knob" value of these requirements. These guidelines allow project managers and personnel to understand the issues involved in order to allow tradeoffs to be made. The failure modes generated for each requirement feed directly into the third task, Defect Detection and Prevention [Ref. 2], which utilizes the Accurate, Cost-Effective Qualification (ACEQ) engine [Ref. 3] to systematically correlate these failure modes, or risks, with the mission requirements. This process results in a matrix of weighted influence coefficients, When mapped against the various PACTS and weighted by efficacies and resource requirements, a ranked list of PACTs is generated from which project personnel can tailor the assurance program for a particular mission. The fourth task, Technology Readiness Assurance Guidelines, identifies unknown effectiveness parameters, assesses the readiness of a new technology to be inserted into flight projects, anti identifies focused research efforts into potential risk elements. This task provides the assurance status and need for infusion of new technologies into the New Millennium Program (NMP).

6. Guideline Description

The guidelines described in this paper deal with the product assurance aspect of the requirements for a project. Each guideline focuses on a PACT typically used to screen for specific potential failure modes, Screen is used here in its most general sense, i.e. a product with potential or actual failure modes is dropped through the "screen" and a better product emerges (see the "waterfall chart" in Figure 2). A list of predominant failure modes relevant to each guideline is also generated. In most cases they are supported by results of searches from ground test and in-flight problem/failure databases for JPL and GSFC flight missions, Cost drivers in the performance of these specific PACTS are identified for potential tradeoff **studies.** Parametric tradeoffs that would be cost effective are indicated. **In addition, effective** substitutes for specific PACTS are identified.

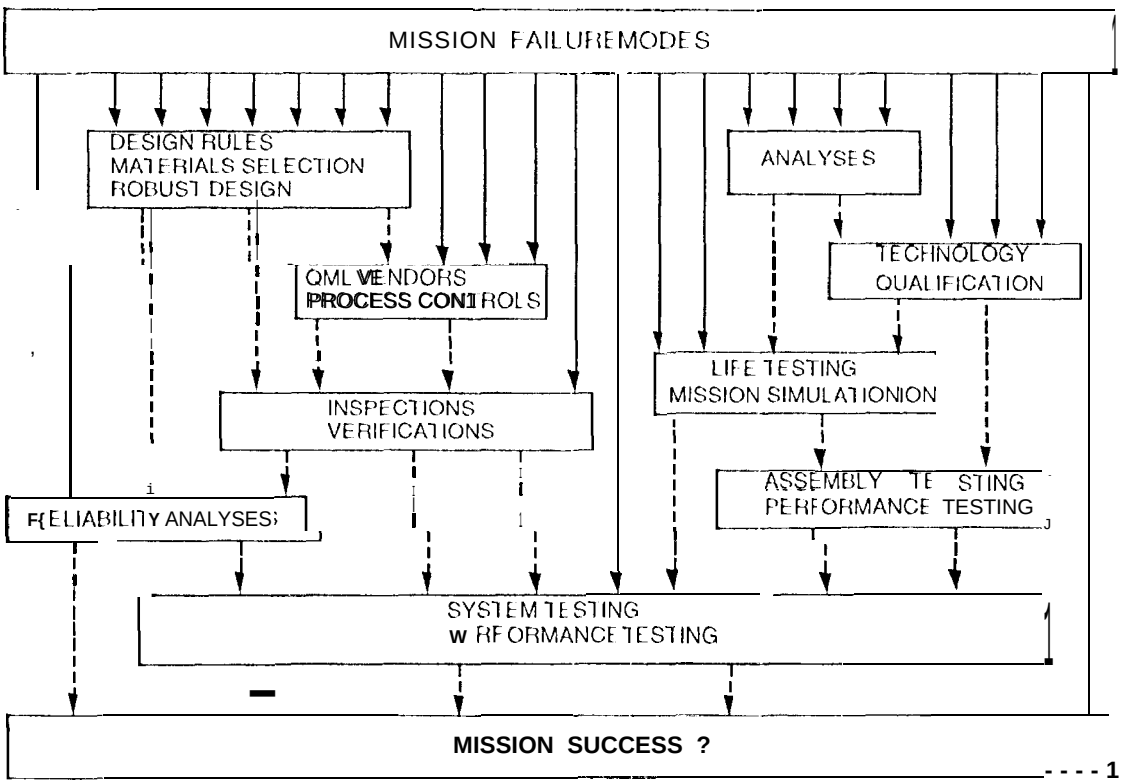

Figure 2. The "waterfall chart" showing the different types of PACT screens to prevent failures from occurring in flight.

Each guideline succinctly and precisely describes the objectives of the particular PACT. I-he typical requirements of the PACTS used on current projects are then listed. This allows an evaluation of the necessity of some elements of the requirements and the level of risk associated with a reduction of selected elements as described below.

In the past the rationale for imposing some requirements has not been well documented and there have been confusions as to their usefulness. In these guidelines the rationale for each PACT is clearly described and listed, This again allows the risk to be identified and evaluated. The relevant failure modes that the PACT seeks to address are also listed. This includes only predominant failure modes that have been documented by ground test and in-flight problem/failure databases for JPL and GSFC flight missions. The guideline follows with a description of the method by which the requirement is applied.

Having listed all the background information, it is now ready for the trade-offs, The control parameters to which the PACT is sensitive to are identified. A plot of failure modes as a function of these parameters is plotted to show the sensitivity the failure modes have from changes to these parameters. These parameters can be thought of as a functional knob on an instrument that one can vary to test the sensitivity of a parameter variable to particular failure modes, or risk elements or "knobs". This is a powerful tool in determining the effectiveness of the PACT elements for possible trade-offs. Another important parameter in the matrix is the cost of adding or varying the PACTS control parameters. The matrix also includes the cost sensitivity of increasing or decreasing the parameter. A parameter that is effective in identifying certain failure modes may not be included if the cost is prohibitive. However, other reduced cost options may be available which are focused on that particular risk element, Both parameter sensitivity and cost have to thus taken into account in the trade-off process,

Table 1 - Control Parameter and Cost Sensitivities for the temperature design requirement.

Control Parameters	Failure Modes	Failure Mode Sensitivity to Control Parameters			Cost Sensitivity to Control Parameters	
		T	in spec	surv		
Temperature Levels (T)	Structural/packaging	+	+	+	Temperature Level	0 (1)
in-Spec Range (in spec)	Electrical performance /parameter variation	+	+	0	in-Spec Range	0 (1)
Survival Range (surv)	Optical performance	+	+	0 (2)	Survival Range	0 (3)
	Time dependent failures (Arrhenius)	+	0	0		

(1) Not a cost driver over typical temperature ranges (-20/+70 'C). RF and optics assemblies may have cost impact due to strong temperature sensitivity of their performance.
(2) Survival temperature is not a driver, unless the range is wide enough to cause permanent change in the optics structure.
(3) Not a cost driver unless effect mentioned in (2) is an issue.

As an illustration of this technique, Table 1 shows a simple example of a matrix of control parameter sensitivity and cost sensitivity for temperature design requirement, Column 1 lists the variables (control parameters) in temperature design: temperature level, in-specification

temperature range, and survival temperature range. The top level generic failure modes associated with temperature design requirement are related to: structural and packaging issues, electrical performance and parameter variation issues, optical performance, and time dependent failures. These failure modes are plotted as a function of the control parameters in a matrix. A "-t" indicates that the perceptiveness to a failure mode is increased by an increase in the parameter. This matrix shows that time dependent failures, for example, are more easily precipitated by an increase in temperature. A "0" indicates that varying the control parameter has little or no effect on the failure mode. A "-" would indicate a failure mode not being easily precipitated by an increase in control parameter values. 1 he matrix on the right shows the cost impact on the three control parameters. For typical temperature ranges, these control parameters are not big cost drivers, unless the range is so great as to cause permanent changes in the system.

7. **Conclusions and Discussion**

The Risk/Requirements Tradeoff Guidelines have been assembled in a document [Ref. 4] for FBC missions. It summarizes the reduced-cost approach for the design, verification, and validation of flight equipment for assuring mission success of microspacecraft or low cost missions.

The first and second editions (Rev. A and B) of the document contained guidelines for a subset of product assurance activities that have been deemed critical in a recent study to prioritize them. 1 he latest, third edition (Rev. C), of the document contains more product-assurance guidelines from the prioritized list. Additional guidelines, as part of the ongoing effort, will be included in future revisions. These guidelines are self-optimized in the parameters to whose variance they are sensitive. In order for the entire product assurance program to be optimized, the guidelines need to be optimized with respect to each other, Optimization between related disciplines (e.g. dynamic, thermal, analysis, etc.) will be made from existing guidelines in the next revisions and become more possible as the number of guidelines generated is increased. Subsequent revisions will involve optimization across disciplines and for combined disciplines. This document is intended to assist projects in their FBC efforts, thus the guidelines will be periodically revised and updated to reflect the changing needs of future missions.

8. **Acknowledgments**

The work described in this paper was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under contract with the National Aeronautics and Space Administration (NASA). It was funded by NASA Code QT under a Research Technology Operating Plan (RTOP). We are grateful to Mr. Tom Gindorf, Manager of the Assurance Technology Program Office, for his **initial** involvement in starting up this task and his continuing support. We are also grateful to the New Millennium Program for their willingness to "revolutionize" all aspects of the product development cycle.

I-his document is the product of the efforts of a number of personnel within **the Office of Engineering and Mission Assurance at JPL,** including Reliability Engineering, Quality Assurance, and Electronic Parts Engineering Offices. Each guideline may be the work of one or more contributors. Their efforts are greatly appreciated.

9. References

1. "Risk as a Resource - A New Paradigm", M. A. Greenfield and T. E. Gindorf, Probabilistic Safety Assessment and Management '96, ESREL'96/PSAM -111, Crete, Greece, June 24-28, 1996, Eds. Carlo Cacciabue and Ioannis A. Papazoglue, Vol. 3, pp.1 597-1605 (Springer, New York, 1996).
2. "Defect Detection and Prevention", Steven L. Cornford, 16th Aerospace Testing Seminar, Los Angeles, March 1996.
3. "A Systematic Approach to Qualification", Phillip R. Barela and Steven L. Cornford, Proceeding of the Institute of Environmental Sciences, PP.118-126, 41st Annual Technical Meeting, Anaheim, California, April 30-May 5, 1995.
4. "Risk/Requirement Trade-Off Guidelines for Faster, Better, Cheaper Missions, " Kin F. Man, Editor, Jet Propulsion Laboratory Report (JPL internal document), JPL D-12441, Rev. A, B, C, January, April, July, 1996.