Risk As A Resource - A New Paradigm

Dr. Michael Greenfield
National Aeronautics and Space Administration
Washington, D.C.

Thomas E. Gindorf
Jet Propulsion Laboratory
California Institute of Technology
Pasadena, CA

INTRODUCTION

NASA must change dramatically because of the current United States federal budget climate. The American people and their elected officials have mandated a smaller, more efficient and effective government. For the past decade, NASA's budget had grown at or slightly above the rate of inflation. In that era, taking all steps to avoid the risk of failure was the rule. Spacecraft development was characterized by extensive analyses, numerous reviews, and multiple conservative tests. This methodology was consistent with the long available. schedules for developing hardware and software for very large, billion dollar spacecraft. Those days are over. The time when every identifiable step was taken to avoid risk is being replaced by a new paradigm which manages risk in much the same way as other resources (schedule, performance, or dollars) are managed. While success is paramount to survival, it can no longer be bought with a large growing NASA budget.

NASA's *better, faster, cheaper* philosophy for doing business will provide the foundation for an exciting space program that delivers more tangible value in products and more relevance to the public at significantly lower cost. Pivotal to the success is a new approach to product assurance. The challenge facing NASA today is not failure avoidance at any cost, but rather reengineering our processes to reduce the cost of success.

in the new NASA, risk management must be developed as a skill to a far greater degree than has existed in the past. Past approaches have produced great successes but at great cost anti lengthy schedules. In the future, risk and its component contributors must be re-evaluated. There are three contexts of risk that will be addressed in this paper: *risk as a resource*, which expands and shifts traditional risk considerations; *marginal cost of risk*, which addresses the cumulative anti time related effects of risk reduction; and, an alternate definition or *new meaning of success and how* it relates to risk.

Risk as a Resource - Risk in the new NASA must be considered *a priori* as an expendable and managed as a resource just as mass, power, performance, schedule, and cost are resources. In the past, risk management frequently meant that a project was managed either not to take risk or to minimize risk (always at considerable cost). Given enough time and money, risk can be reduced to near zero. As a natural product of' this successful past, a pattern has developed to take very little risk by applying over 35 years of accumulated test and analysis experience to today's technology. Spacecraft development has characteristically added additional analysis and testing as each new one was developed. Over-conservatism is the product of this tradition. Such conservatism is no longer economically feasible, nor necessary with today's significant advances in process control and reliability.

Mass is a resource that is traded against funds available (to develop alternative approaches) and mission objectives (launch capability to trajectory Insertion). Power is a resource that is traded against funds available (lo develop alternative approaches) anti capability (electrical, thermal, etc.). Similarly, risk is a resource that must be traded against funds and schedule available (to test or analyze) and confidence.

When risk is viewed as a resource instead of a consequence, the cost of risk reduction can be minimized through intelligent application of tradeoffs. This statement is loaded with challenges. *Risk m a resource* instead of a consequence infers an ability to *a priori* understand and articulate the results of actions taken or not taken and (heir cost. *Intelligent application of tradeoffs is* another loaded phrase. At the heart Of effective consideration of risk is the innate ability to discern, based on as much available information as can be efficiently obtained, what the course of action should be. In today's technical environment, feelings regarding risk have little to do with success. The challenge to the reliability community is to understand and articulate the results of actions taken and their associated cost. Later in the paper, a failure assessment approach and a risk requirements tradeoff approach to provide these needed understandings are discussed.

Marginal Cost of Risk - To be effective in the future, approaches that *realm the cost of success arc* needed. A simple way to express reducing the cost of success is as a relationship in which the cost for further risk reduction is determined to greatly exceed the value of reducing it. Borrowing from general economic theory, this relationship has been labeled by the authors as the marginal cost of risk.

MARGINAL COST RISK

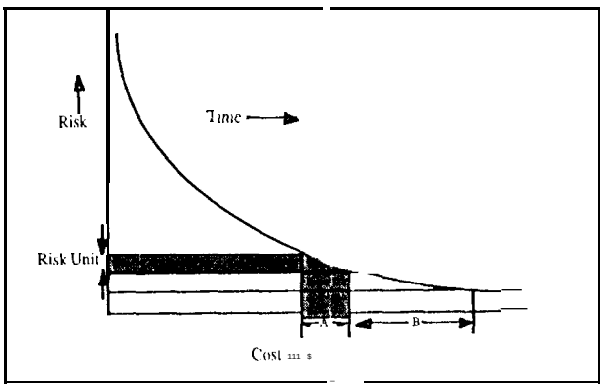


Figure 1

In Figure 1, one observes that the incremental reduction of risk comes at increasingly greater cost (f I> A). The marginal cost of risk is the difference between B and A. For equal reduction in risk early in a program, the cost difference between adjacent equal units of risk (normally measured as probability of survival) is not large. As lime progresses and risk is reduced further, the incremental reduction of risk becomes increasingly expensive. As a project development matures, the. early application of resources to a judiciously selected assurance provision is much more c. ffective in reducing risk than a later application. It is on (he proper selection of risk control measures and appropriate phasing of resources application that ultimate risk to mission success and the cost of controlling it depend.

New Meaning of Success - Productivity in the space "business" concerns the number or percentage of successes pcr unit cost (or successes within a specific period of time). Productivity in space will never be 100%, and furthermore, should not need to be. Often in the past, every payload launched was viewed as a single event uncoupled to other payload launches. In tile future, a shill is needed to think of space enterprise productivity in terms of programs; i.e., a series of events and not as discreet occurrences. Programs can be considered as a set of events for which satisfaction is achieved by an accumulated high percentage of successes. When viewed this way, program objectives accomplishment replaces single element successes or failer-cs. As an example, a program objective to observe the earth's weather patterns is not dependent on a single element for success. 1 n fact, meteorological satellites in an array may have deficiencies in the individual elements, including total failure of a sensor; hut, if the sky is mapped, the program objective is accomplished and the program is considered a success. 10 fact, replacement spacecraft are anticipated anti readied as needed to maintain program objectives. When success is viewed in this way, the management of risk for a program is allowed much more latitude in dealing with risk control rather than risk avoidance. This has significant cost bene fit.

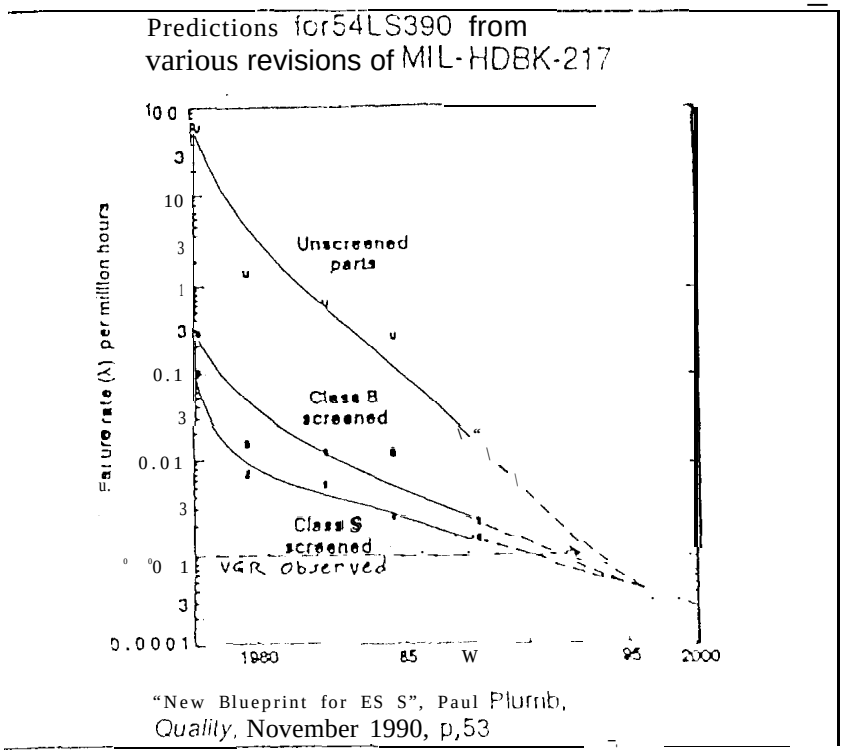
NEW APPROACHES

Innovative approaches in ail assurance disciplines must be instituted. Simple, cheaper, but effectual reviews must be developed. Instead of large gatherings before astute groups of managers, concurrent peer reviews at all levels of assembly by technical experts should be conducted to determine and resolve issues in real time. This is *better*. Innovative test approaches, where oniy significant value-added testing is performed, are needed. This is *faster* and *cheaper*. Analysis must be done only where true value is gained. Erudite arguments arc often presented on necessity of analysis, but ncw discipline in determining anti doing only those analyses which are real I y necessary must be established.

Design - Design practices traditionally followed may not fit today's *better, faster, cheaper* environment. Design trades arc a kcy place for cost savings and a great opportunity for innovation in successful risk management.

An example of traditional low risk design is the. requirement to usc oniy the highest reliability paws. However, in 1996, this traditional approach is not as rigorously defendable. When one uscs established commercial parts which have been in high volume production under statistical control, advantage can be taken of the advances in modern manufacturing controls and technological progress. From Figure 2, it is seen that commercially available parts of i 996 can be projected to have reliabilities of the same order as Class S parts of 1977.

This leads onc to consider the possibility that the two Voyager spacecraft launched i n 1977, made predominantly of conservative applied and highly screened parts (≥ Class S), both of which arc still operational after i 8 years, could be built in 1996 with commercial parts with anticipation of similar reliability.



"New Blueprint for ES S", Paul Plumb, *Quality*, November 1990, p,53

Figure 2

This bold advance in capability would significantly reduce parts' costs (between 4- 10X) and parts acquisition time (by 2X). The reliability improvement depicted in Figure 2 is mainly attributable to the fact that manufacturing capability has improved such that the extensive parts scrutiny to weed out poorly manufactured parts and to achieve Class S status in 1977 are no longer necessary to expect a similar capability.

Do not be misled by this example. If the Class S scrutiny were applied to 1996 parts, the result would be parts more reliable than simply acquired commercial parts. However, the question is, does that reduction in risk justify the cost and schedule consequence? in 1977, the answer was yes. In 1996, the answer is dependent on the consequence of the risk. For an unmanned four-year planetary mission like Voyager, the answer today would be no. For a manned mission where a critical subsystem affects human life m critical military applications, the answer could still be yes. The ability to decide which risks are acceptable in the light of the consequences of failure crystallizes the real issue of risk. Just as mass cannot exceed the launch capability, or power demand cannot exceed that available from the power source, so also risk is a resource which cannot exceed the perceived cost of loss (or consequence) due to failure. It is this balance between the cost of failure and the risk taken that is the essence of risk management. Since the consequence of managed risk is either performance success or failure, the consequence of failure must trc understood and mitigated to the appropriate degree, but not to an absolute minimum except irr rare cases.

Advances in process control and technology as described above need to be carefully understood and the previously applied test, analysis, and methods of review changed accordingly.

Testing - The NASA Office of Safety and Mission Assurance is funding, an effort to learn the lessons from past testing experiences as well as develop innovative new methods for qualification and acceptance testing. This effort is called the Test Effectiveness Program.

An example of innovative testing approaches is synergistic testing. Reducing serial test events which have significant schedule and cost consequences to a concurrent or at least parallel set of activities as well as deferring some test to the system level is one way to do things *faster* and *cheaper*.

The consequence of a set of discrete serial events is high cost, long schedule, but low risk. It is possible, with some deferred and moderately increased risk, to greatly reduce cost and schedule. This is a type of consideration needed if the future assurance provisions are to be "in sync" with decreasing spacecraft budgets.

Risk Evaluation - In order to structure a new way of addressing risk, the NASA Office of Safety and Mission Assurance has sponsored a triad of activity addressing assurance requirements. In Figure 3, intelligent risk decisions (A) are made by considering the consequences of alternate levels (B) and the value of the imposed product assurance provision in detecting or preventing critical failures (C).

The Risk/Requirements Tradeoff and Tailoring task (B) reflects on the parametric sensitivity of control parameters to the effectiveness of the assurance provision imposed. Consider implementation of a recognized standard test. Strict imposition of a standard test may drive design cost, test implementation cost, or problem resolution cost unreasonably. Any one of these consequences would also likely affect schedule. Prudent modification Of a standard test is facilitated by the intelligence provided in the Risk/Requirements Tradeoffs and Tailoring Guidelines (B).

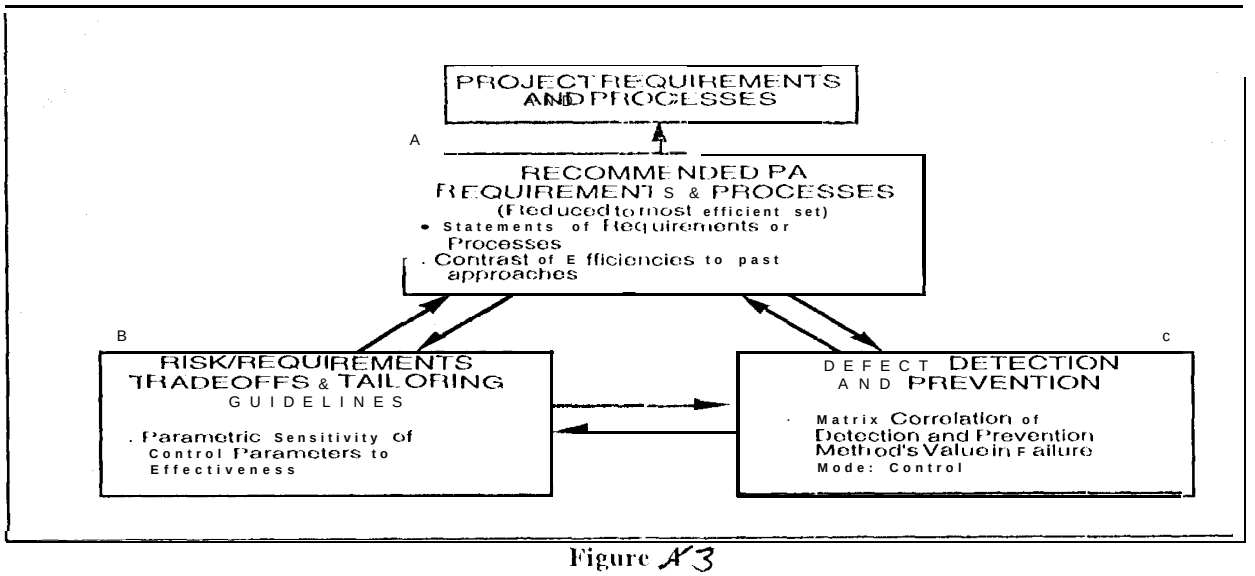


Figure A3

These modifications should seek to accomplish the intent of the original test but factor in the avoidance of unnecessary cost and schedule impact. For example, for electronics, the technical details of the effect of a thermal test at "standard" temperature T_1 and duration t, (which is predicted to be marginal in terms of overstressing hardware) can be correlated to a less stressful test at T_2 slid t, in terms of the change in failure rates. Consider an Arrhenius type failure typical in electronics such as typified in Figure 3.4

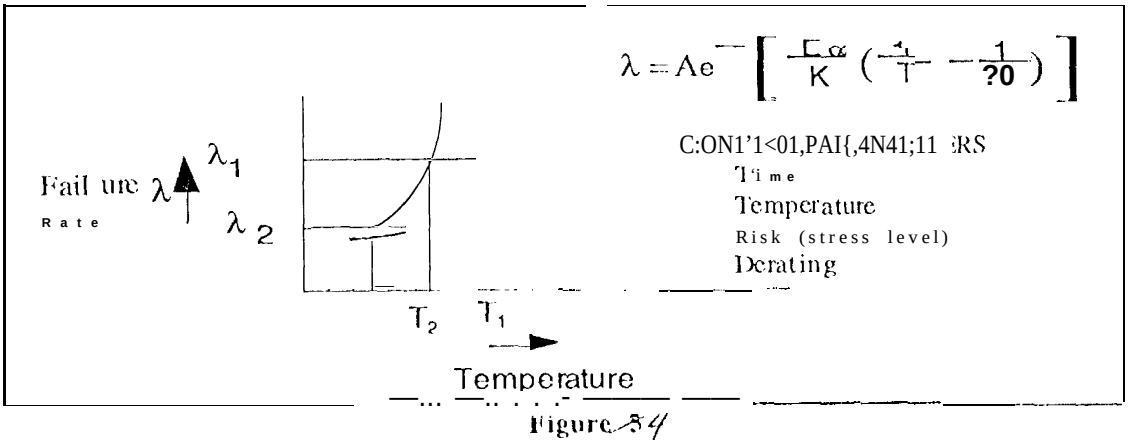


Figure 3.4

Clearly, λ decreases as temperature is lowered from T_1 to T_2. in order to see the same number of failures as expected at „, the test would need to be increased in length. By this approach, the same effectiveness of failure detection could exist for a lest at '1'$_2$ as at T_1 as long as the lower temperature did not move below the threshold for which temperature activates a specific failure mode. The method for detecting whether or not the physics of failure was compromised by the lower temperature '1'$_2$ testing would be determined by applying the Defect 1 Detection and Prevention (C) process.

The Defect Detection and Prevention (C) task has as a cornerstone the dc.termination of the effectiveness and relative value of various assurance activities; i.e., Preventions, Analyses, Process Controls, and Tests (PACTs) to detect and/or prevent failure modes from jeopardizing mission success. in Figure 5.6, one. can visualize failure modes as being detected, prevented, or missed by various PACTs. In the figure, clearly some failure modes may be detected by any one. of a series of PACTs. This can be very costly if all are performed. The key is to eliminate redundant screens without unduly compromising detection and jeopardizing mission success.

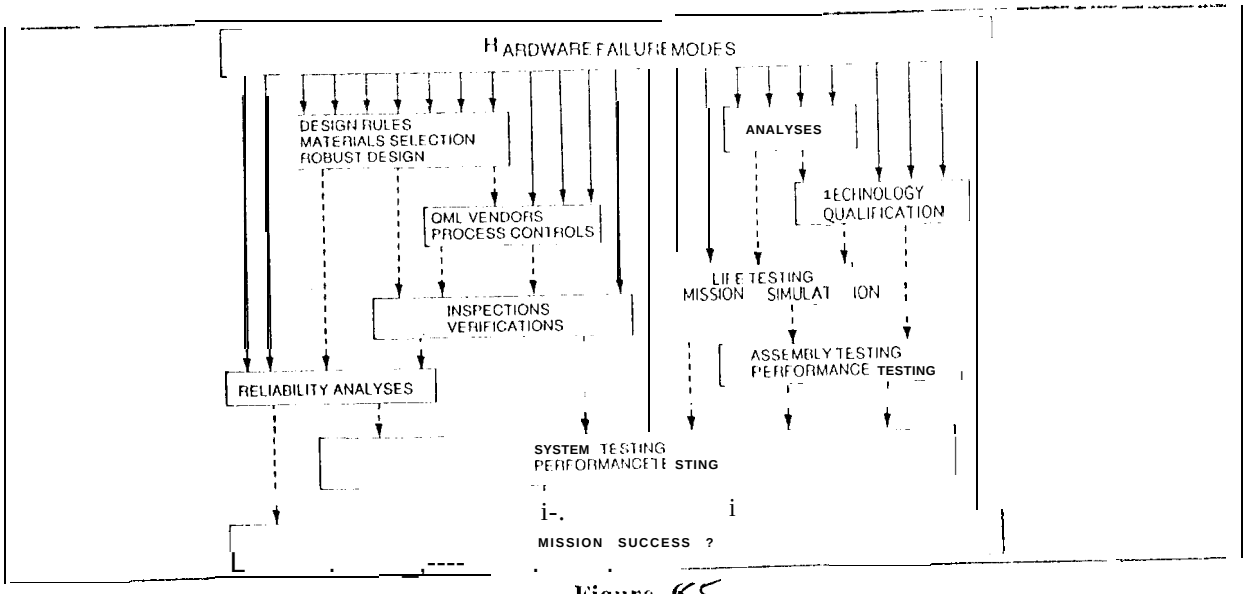


Figure 5

A mechanism for evaluating the relative value of a given Prevention, Analysis, Control, or Test (l'ACl') as an assurance mechanism for failure mode avoidance or control was developed by Barela and Cornford at JPL [1]. '1'1 ic mechanism developed is called Accurate Cost Effectiveness Qualification (ACEQ) and can be simply characterized i n a summary sense by the matrix found in Figure 6

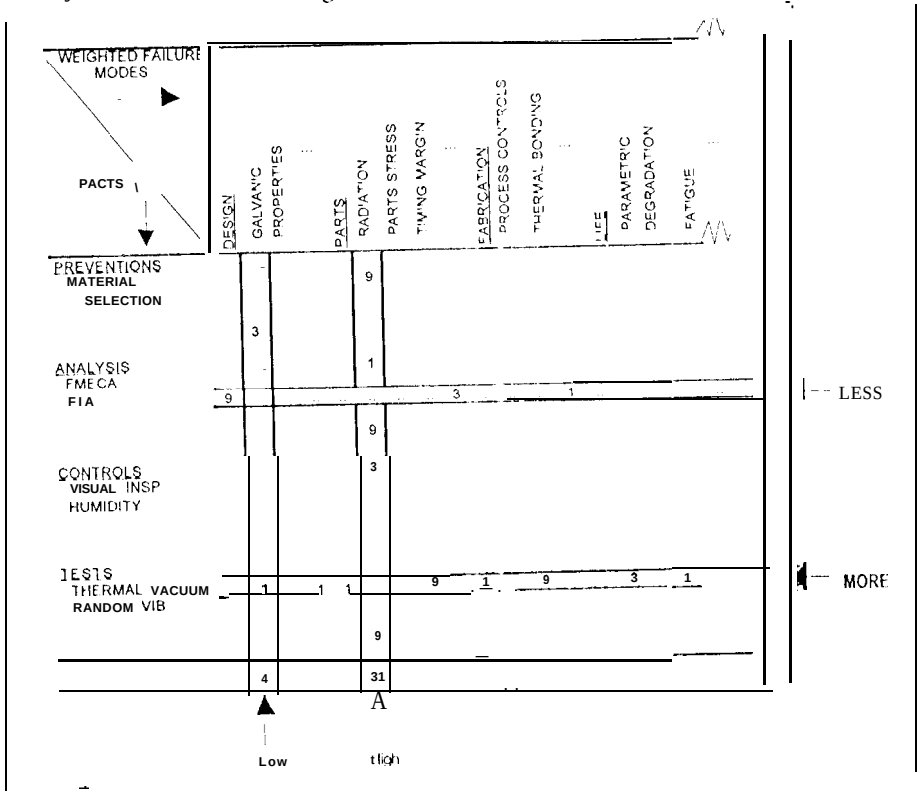


Figure 7 - ACEQ Matrix

In Figure 7, one observes that all known failure modes (columns) arc assessed versus the various PACTs. These failure modes are weighted by likelihood of occurrence and impact on the mission. A simple rating scheme for screening effectiveness consists of applying a weighting system where a value of 1 implies very little effectiveness, 3 implies a model-ate degree of effectiveness, and 9 implies a high degree of effectiveness.

References

1. Cornford S. 1., Barela 1'. R.: A Systematic Approach to Hardware Qualification. IES ATM proceedings, 1995

When applied, the rating scheme permits a correlation along the relative effectiveness column that points to whim combination of PACTs have the most effectiveness (value) in detecting failure mode. Costs of the PACTs can also be included and correlated to effectiveness in the ACEQ process. Correlation along the relative detectability row points to the degree to which a particular failure mode is addressed for a particular set of selected high value PACTs.

As an example, carrying through with the previous thermal discussion, it is **practical to** correlate the effectiveness **of a thermal** test as a screen for failure modes at a given temperature (T_2) by contrasting how the different temperature levels affect the various failure modes. This physics of failure assessment is embedded in the ACEQ technique.

The thermal example discussed is greatly simplified for illustrative purposes of the risk assessment process. When fully developed for a myriad of assurance elements, the combination of understanding the effectiveness of the assurance provisions control parameters and the relative value of any one assurance provision compared to others is a powerful tool with which to manage risk control. The approach described is being developed and applied to NASA's New Millennium Project. The output of the activity will be useful to spacecraft designers for a broad army of applications. The significance of and ability to tradeoff preventions, analysis, controls, and tests allow cost and risk to be managed appropriately.

Mission Success - The meteorological satellite discussion addressed a new meaning of mission success; i.e., judging success as accomplishment by a series of spacecraft addressing mission program objectives rather than by any one discrete spacecraft. This approach fits the context of several new NASA programs. The New M i] lennium Program is a series of small space.crafl launched on short schedules to demonstrate emerging technologies. Success here is not dependent on any one spacecraft accomplishing tbe entire program's mission objectives. A similar scenario exists for the Mars Exploration Program where an array of spacecraft are being developed to accomplish a variety of objectives. Again, any one spacecraft dots not carry the full burden of' mission success, since it is the total program against which successshould be judged. Therefore, a key consideration which provides impel-tant latitude in the *better, faster, cheeper* environment is the degree to which ao individual spacecraft in a series of spacecraft must avoid risk, i.e., be failure proof. A key ingredient in evaluating the required quality of a spacecraft is the prediction of the probability of survival R(t). Today, reliability predict ions are marginal at best. Once the credibility of predictions is established, risk management will have an invaluable tool to trade risk as a resource. Confidently being able to predict probability of survival would greatly simplify and quantify risk/cost trades. For example, consider whether it is better to launch one expensive very iow risk (R(t) ~.99) spacecraft or to launch four moderate risk (R(t)~.8) spacecraft. The higher risk spacecraft can be developed in shor ter time periods for less cost. In tbe first case, there is enormous expense to optimize reliability **for an** expectation **of onc** success. In **the** latter **case,** there is expectation of three successes (and one failure), but at moderate cost because every prevention against failure is not exercised. It is recognized that no one likes failure. One could view R(t)~.8 as ter rible if the overall *value of return on* cost of the program wasn't thoroughly considered, planned for, and accepted. This example obviously requires ability to predict sur vivai (R(t) and the avoidance of systematic common mode failures. Avoidance of systematic common mode failure, consequently, is a critical place to focus the precious **risk** management **resources.** Does this sort of conceptualization encourage failure or promote a flippant attitude toward failure? NO! This conceptualization promotes minimizing the cost of success.

SUMMARY

Risk is a complicated issue. in the series spacecraft examples discussed, several important elements have to be considered in developing the program's risk logic. These include: cost (meteorological satellites are relatively inexpensive); consequence of failure (in these unmanned missions, human life is not endangered by failure of an individual spacecraft); and success (some is always guaranteed). The. taxpayer wiii accept risk trade-offs in [his environment. In the future, all aspects of cost must come down. New efficiencies must be developed. Tradition and yesterday's answers aren't necessarily right for today's technologies; e.g., the previous example of a Voyager class spacecraft in i977 vs. 1996.

A new attitude to consider assurance provisions that add value anti provide adequate, not optimal, confidence is a challenge that the reliability community needs to accept. While success is necessary for **survival,** affordability **is a** mandate. Risk **management** should embrace new tenants and develop clear, succinct ways to ar tic ulate the concepts which help projects to balance risk as another basic resource.

Risk management **must bc** forward **looking** and progressive, not tied to the traditions of past assurance methodologies except where those methods arc both technically and cost effective. The future Of NASA will be tied to its efficiency and productivity. Risk avoidance must be an axiom of the past; it simply cannot be supported in today's economics. Systems processes must be reengineered to methods which understand and manage the risk resource without precluding a high expectation of success.

ACKNOWLEDGMENT

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