JOURNAL OF SPACECRAFT AND ROCKETS
Vol. 41, No. 1, January–February 2004

Risk Chair for Concurrent Design Engineering: Satellite Swarm Illustration

James L. Benjamin* and M. Elisabeth Paté-Cornell†
Stanford University, Stanford, California 94305-4026

Whereas concurrent design engineering (CDE) processes show great promise for reducing design time and cost, the implicit management of technical risk raises questions about the reliability of resulting designs. CDE team members (chairs) may not possess the skills to perform risk assessment. The authors propose that a risk analyst be integrated into concurrent design engineering teams to explicitly manage a design objective. The contributions that such an analyst could make in the aerospace industry and the tools and information that would be needed to support real-time analysis are discussed. A terrestrial observer swarm problem illustrates the top–down approach to technical risk assessment during the concurrent design process. The swarm model is analyzed in increasingly adaptable models, starting with an instant dual-redundant system and ending with a discrete-time Markov model of swarm life involving dependent satellite lifetimes and an uncertain number of satellites due to the possibility of failures of launch and dispensing operations.

Nomenclature

D_i = daughter satellite i, where i is $1, 2, \ldots, n$

F_i = event that D_i fails during a given time period

$\bar{F}_i$ = event that D_i is working during the same time period

F_i, F_j = joint event that both D_i and D_j have already failed at a given point in time

$Pr\{A\}$ = probability that event A occurs during a given time period

$Pr\{A|B\}$ = probability that event A occurs given that event B has occurred

p_j = probability of the jth failure among n daughters, that is, $Pr\{X_i = n - j | X_{i-1} = n + 1 - j\}$

q_j = probability that the mother satellite fails after $j - 1$ daughters have failed

X_k = number of daughter satellites working during discrete time period k

Introduction

THIS paper discusses the addition of a risk analysis specialist (a risk chair) to concurrent design engineering (CDE) teams and presents tools that can make such a specialist effective. The design of space systems has evolved in recent years to embrace the CDE process to achieve rapid convergence on choices of equipment and configuration to meet mission requirements. CDE teams implicitly manage reliability, first by limiting component choices to those which the mission sponsor deems to be space qualified and, second, by using rules of thumb to judge which parts will perform reliably yet efficiently during the mission. Explicit quantitative engineering reliability assessment is deferred to a later design stage, when more detailed specifications are available.

Whereas the CDE process shows promise for reducing design time and cost, it raises questions about the quality of design reliability decisions. The sponsor, managers, and engineers who participate in the design exercise quickly and tacitly inject their individual values into decisions about what failure risk is acceptable and what parts are deemed reliable enough. Their individual judgments may or may not be collectively consistent. The same process takes place at an organizational level: Engineering disciplines that measure (or corporations that anticipate the measurement of) performance according to that of their component may train their representatives to overspecify these parts so that, when the satellite fails, fault is assigned elsewhere.

CDE team experts (chairs) skilled in controlling mass, power, or other budgets may not be as skilled in risk assessment techniques. Therefore, explicit risk assessment, if performed at all, is often delayed, and by the time it is conducted (generally bottom–up) on an engineering design that is detailed enough to be perceived as credible, considerable amounts of time, money, and effort have been spent. These expenses raise the cost-benefit hurdle that proposed design changes must clear. Such hurdles can cause some faster–better–cheaper designs to be less reliable than similarly budgeted alternatives, whereas other designs may unnecessarily sacrifice money, schedule, or functionality to achieve high reliability goals that may not efficiently contribute to the reliability of the overall system.

These concerns invite the question of whether reliability engineering can be integrated into the concurrent design engineering process to produce cost-effective designs that achieve explicit reliability targets. We advocate that a risk analyst using probabilistic risk analysis (PRA) techniques, based on systems analysis and probability, be added to the team to manage a budget of satellite design risk. This approach is illustrated here by the design of a swarm of satellites.

Extensive research has been devoted to reliability engineering in high-cost, high-risk fields. Stochastic models are a staple of safety engineering in process industries.[1] However, the application of these methods to highly customized, low-cost satellites is relatively new. The U.S. Department of Defense (DOD) has an obvious interest in reliable engineering systems. The DOD has specified methods to assess military electronic system reliability[2] and has determined the reliability measures to be used by designers of electronic systems.[3] Hecht and Hecht observed that then-current methods of predicting spacecraft life have overestimated failure rates,[4] resulting in satellites such as Pioneer 10 that have exceeded their intended life.[5] Although this longevity may be a happy outcome for the payload stakeholders, and may simply be due to randomness in component performance, the objective of exceeding mission lifetime should not be part of design criteria because excessive allocation of resources to one project can preclude the funding of other worthy projects. Other space-oriented agencies have published their own handbooks documenting reliability engineering philosophies.[6,7] Failure mode and effect analyses provide a qualitative basis for ranking risks, but

Received 16 January 2003; revision received 7 May 2003; accepted for publication 12 June 2003.

*Ph.D. Candidate, Department of Management Science and Engineering. Student Member AIAA.

†Professor and Chair, Department of Management Science and Engineering.

not a quantitative means of assessing the robustness of possible solutions. Bourret and Reggia have proposed methods of collecting data to diagnose the causes of satellite failures.[8] Loll has described a way to allocate reliability budgets across the components of an electronic systems,[9] and Mosher et al. have discussed the need to reconcile reliability with the faster–better–cheaper trend.[10]

Another influential line of research has focused on the use of conditional probabilistic methods to analyze design decisions that affect system reliability. The basic methods of decision analysis, including assessment of the cost effectiveness of additional information, are presented in classic readings in decision analysis.[11] Lowell applies conditional probability to decision problems,[12] whereas Keeney and von Winterfeldt show the importance of obtaining explicitly expert opinions to assess these conditional probabilities.[13] Barlow discusses the limited applicability of traditional stochastic methods to finite population problems and proposes treatment of conditional probability in reliability engineering using such tools as decision and influence diagrams.[14]

Widely read aerospace engineering texts summarize traditional approaches to reliability engineering (e.g., Hecht[15]), but techniques for assessing the reliability of space systems are evolving. Laube studied the impact of ground storage on component reliability.[16] Linton developed closed-form reliability solutions for parallel redundant systems of n components ($n > 4$) with constant failure and repair rates.[17] Weibull and other analytically tractable distributions have been used to assess the reliability of individual hardware components such as radar sensors,[18] batteries,[19] attitude control systems,[20] and solid state recorders[21]; however, the treatment of software reliability is more challenging.[22] Paté-Cornell and Fischbeck presented a framework based on PRA for reducing the risk of losing space shuttle vehicles and crew due to failures of the tiles of an orbiter's heat shield.[23] Estimated maintenance costs for a preliminary design of the space station were analyzed probabilistically by Fragola and McFadden.[24] Guarro adapted PRA techniques to assess the safety of the nuclear-powered Cassini space probe mission.[25] Frank pointed out the importance of linking PRA of space systems to design decisions.[19] Rasmussen and Tsugawa simulated the lives of a collection of identical satellites containing components with fixed expected lifetimes to assess how satellite size affects the usefulness of constellation architecture.[26] Risks of collision with space debris were analyzed by Walker et al.[27] and by Paté-Cornell and Sachon.[28] Guikema and Paté-Cornell warned of pitfalls awaiting space program managers when project teams' politics drive the allocation of resources.[29] They also proposed a method to optimize the allocation of resources to minimize the failure risk.[30] Walton and Hastings suggested using portfolio theory to model and prune the high-level architecture tradespace.[31]

There are also efforts to gather data for parts that have failed in flight into a database that will allow designers to update their assessments of component reliability. Thaggard reported on such a project for NASA.[32] Helgevold and Crosse summarized the report of anomalies for seven satellites.[33] More recently, Lee et al. described a project of The Aerospace Corporation to create a database and access methods that can be used to update initial assessments of component reliability based on flight experience.[34] This work updates an earlier effort by Neogy and Siu.[35] Concurrent engineering has been the subject of many reports (e.g., Hoffman[36]). Guarro pointed out that PRA originally fledged in aerospace before finding acceptance in nuclear engineering (and now in the space industry) and anticipated the possibility of applying PRA to CDE.[37]

The study described in this paper draws on several elements of the research described. Its objective is to incorporate PRA in the work of CDE teams in the aerospace industry, with illustration for the case of a hypothetical terrestrial observation swarm (TOS), composed of one mother and several daughter satellites. When assessments of satellite subsystem performance are combined. into a model of satellite and swarm reliability, the design team can better understand and manage the risk dependencies that stem from common design choices. Systems with known satisfactory reliability levels are analyzed at a coarse level of detail, whereas those that contribute greater failure risk or for which there is less information are recursively decomposed into subsystems with a small number of components. The failure probabilities of each component are assessed, and alternative components that could reduce the overall failure risk are considered. (Note that, although the process of component integration is recognized as an important source of risk, it is outside the scope of this paper.)

The cost of risk analysis is kept low by limiting the number of components that are examined in greater detail and by exploiting conditional independence. (Event A is conditionally independent of event B given event C if $Pr\{A|B, C\} = Pr\{A|C\}$. For example, given a power failure, a telecommunications subsystem failure might be conditionally independent of a solar panel failure because the power failure may account for both problems.) The concurrent engineering team's design software must be enhanced to send reliability information from each existing chair (for example, thermal, power) to the risk chair. The risk chair engineer uses PRA tools to combine the risks associated with other chairs' design choices into a system-level risk assessment. The team's decision makers can then use the resulting risk estimate to tradeoff design risks across components much as they tradeoff mass and power today.

This paper describes and then illustrates the use of risk analysis tools and models by the design of a swarm of satellites. In the second section, roles and responsibilities of a risk chair within CDE teams are described. In the third section, this model is illustrated by the assessment of a satellite's reliability. That section also provides a discussion of when to decompose further a satellite system into its components to improve the failure risk assessment. In the fourth section, a probabilistic model is developed to assess the failure probability of a swarm of satellites over time based on discrete Markov chains.

The sources of risks discussed in this paper are technical because the CDE team that piloted these ideas was focused on technical design. The methods, however, are equally applicable to schedule, cost, funding, and other programmatic risks. If the CDE team includes experts who understand programmatic decisions and uncertainties facing the project, and how these impact the project's value, these factors can be integrated into the method as easily as additional technical components. Indeed, programmatic risk management is the subject of on-going research[38] and may have higher returns than an analysis of technical risk for many projects.

CDE

Overview of CDE

CDE teams try to reduce the chances of schedule, cost, and design errors in two ways. First, design choices with broad implications are quickly propagated across the design team. For example, a higher performance telecommunication component might require greater power. The revised power subsystem might, in turn, increase energy dissipation requirements on the thermal subsystem. If the new components are larger, they can require a larger satellite structure; if mass exceeds a certain threshold, a more powerful launch vehicle may be needed. Such real-time, cross-team reasoning speeds convergence toward an internally consistent preliminary design. Second, the participating customer gets a clear view of the tradeoffs exposed by the CDE process and can quickly communicate preferred alternatives, which are immediately integrated into the design. For example, the customer may hope to increase the value of a mission by employing such a higher performance telecommunications subsystem. The customer can decide whether the benefits are worth the resulting cascade of impacts.

The methods and software tools employed in today's CDE process track mass, power, thermal dissipation, communication bandwidth, propulsion, and many other important design requirements. These current practices certainly make significant contributions to design quality. To the authors' knowledge, however, risk is not analyzed explicitly and quantitatively as part of today's CDE processes. Technical failure risk is closely related to this design process, and is an attractive first candidate for integration of risk into CDE processes.

Today, CDE team members implicitly address reliability requirements across the different subsystems by using rules of thumb to design satellite subsystems. This implicit allocation of resources is likely to be less efficient than an explicit risk-based process. The rules of thumb may not take into account the mission's duration, component load, or other characteristics of the project and may reflect an engineer's reluctance to take the chance of having the subsystem be the first on the satellite to fail. In addition, the small number of well-known component manufacturers has little incentive to share comprehensive histories of part failures with designers because this information increases the market power of customers and facilitates the entry of new suppliers. Finally, rules of thumb are not easily updated to reflect recently discovered failure modes, new materials technology, or improved design methods.

As part of addressing the reliability requirements of customers, aerospace design teams generally complete a reliability analysis of their proposed design before receiving the go-ahead to build. Traditional reliability engineering methods start with a detailed design and compute the reliability of the satellite by integrating the reliability assessments of the components. This computation may assume that the components' lifetimes correspond to analytically convenient distributions, or that they are independent of one another, or both. Imperfect as they are, these analyses are, nevertheless, valued by customers and have played important roles in ensuring quality spacecraft design.[24,25] This poses a problem for CDE advocates: CDE produces a high-level preliminary design and does not generate the detailed input needed for a bottom–up reliability analysis. By the time these inputs are available, the CDE team has generally spent considerable financial and schedule resources and may be required to balance the benefit of changes that reduce technical failure risk with substantial cost increases or delays. Depending on how these factors influence the decision maker's perception of the mission's value, the need for these late redesigns can either reduce or eliminate altogether the benefits of CDE.

Integrating Risk Assessment into Concurrent Engineering

These considerations underscore the need for the integration of quantitative risk management into the concurrent design engineering process even though the details of the subsystems have not been entirely defined. Just as they specify other mission requirements, customers could state a maximum acceptable level of technical failure risk. The CDE team would then be responsible for the choice of components that meet this risk constraint while maximizing the customer's utility. (Utility combines customer preferences for cost, risk, schedule, product capabilities, etc.) If a design satisfying cost, mass, power, faring size, risk, and other constraints cannot be found, the customer can then advise the CDE team which design constraints could be relaxed to make one or more design choices feasible.

The overall reliability of a spacecraft is not an intuitive function of the reliability of spacecraft subsystems. Unlike expected power consumption or mass at liftoff, which are readily derived from the requirements of individual subsystems, the probability of spacecraft survival for a specified period cannot be directly computed by addition or multiplication. Using a simple product of isolated component failure probabilities rests on the questionable assumption that component failures are independent. More realistically, a satellite's probability of failure is a function of component failure probabilities that may be conditioned on the state of other components within (or the environment outside) the satellite. The role of the risk chair that we propose to add to the CDE team is to aggregate and structure these component failure risks and their dependencies into an overall estimate of the mission risk. The risk analyst's task would be to develop and draw on a library of probabilistic models and data that reflect these dependencies among satellite subsystem failures. The risk chair may also have to discover and communicate the customer's tolerance for failure risk.

Model of Swarm Technical Risk

(Swarm of) Independent Satellites

Design Decisions

An integral part of Space Systems, Policy and Architecture Research Consortium (SSPARC) research[39] was to assess the feasibility of a risk chair by creating an analytic reliability model of a TOS of satellites and integrating it into the CDE process. Improved integration with the CDE process drove the following structure for modeling the swarm. First, one needs to decompose the swarm. To parallel the structure of the CDE team, we first broke the swarm into mother and daughter satellites, then decomposed each satellite into its various subsystems. Because corresponding subsystems on mother and daughter satellites are designed by different engineers, the submodels for mother and daughters failure risks are distinct. Second, one needs to consider satellite count. The customer was open to the idea of increasing the reliability of the swarm by adding redundant satellites. Therefore, the number of daughters became an additional parameter of the swarm model, but the similarities in their design (thus, the possibility of a common design error) had to be accounted for. The team eventually proposed a design that included three extra daughter satellites. Third, one needs to account for the probability of reaching orbit. The risk analysis model incorporates a Bayesian analysis of launch vehicles. For each candidate rocket, the probability of a successful launch was modeled using a beta distribution with a prior updated to reflect the outcome of its previous launches. To model launch vehicle capacity limits or to reinforce an operating swarm, the model incorporates the option of a second launch. The model of each launch accommodates up to 2 mothers and 16 daughters and includes a sub-model to represent the risk in the satellite-dispensing phase. Fourth, one needs to provide placeholders for expert assessment of conditional failure probabilities. The reliability of each subsystem is modeled explicitly, but not independently from the others. For example, the successful deployment of a solar wing is modeled as a Bernoulli random variable and conditions the probability of correct power subsystem operation. Similarly, the probability of a successful operation of the payload depends in part on the correct functioning of power, thermal, telecommunications and other subsystems. Because portions of the payload were not disclosed by the customer and the study team members had limited satellite design experience, illustrative lifetime probability distributions were used in lieu of credible expert assessments. Fifth, in the case considered here, subsystems were modeled as either operative or failed because descriptions and assessments of degraded performance were unavailable. However, some subsystems can operate in a degraded mode. In actual implementations, expert insight would permit a more realistic model of the ways in which satellites degrade. In our model, an uncertainty node representing inter-subsystem failure acts as a placeholder through which such intermediate failure states might be represented, until better models are available.

Single-Satellite Model

A satellite's performance depends on the correct functioning of a series of subsystems and mechanisms as shown in the influence diagram shown in Fig. 1. Random variables are used to model the potential failure of considered subsystems. These variables are represented by white ovals such as "Solar Array Gimbal Internal Failure" or "Thermal System Internal Failure." The distributions and parameters of these random variables must be assessed by the responsible

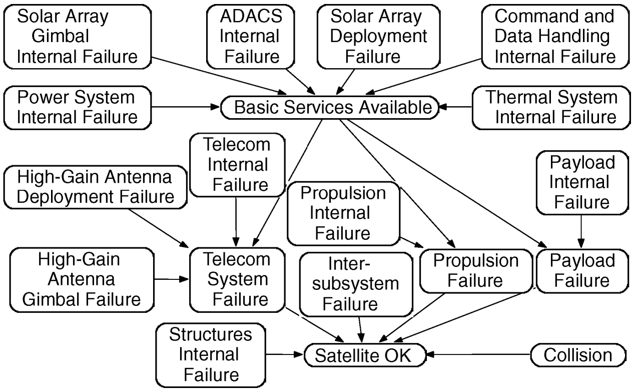
Solar Array Gimbal Internal Failure
ADACS Internal Failure
Solar Array Deployment Failure
Command and Data Handling Internal Failure
Power System Internal Failure
Basic Services Available
Thermal System Internal Failure
Telecom Internal Failure
High-Gain Antenna Deployment Failure
Propulsion Internal Failure
Payload Internal Failure
High-Gain Antenna Gimbal Failure
Telecom System Failure
Inter-subsystem Failure
Propulsion Failure
Payload Failure
Structures Internal Failure
Satellite OK
Collision

Fig. 1 Satellite reliability model.

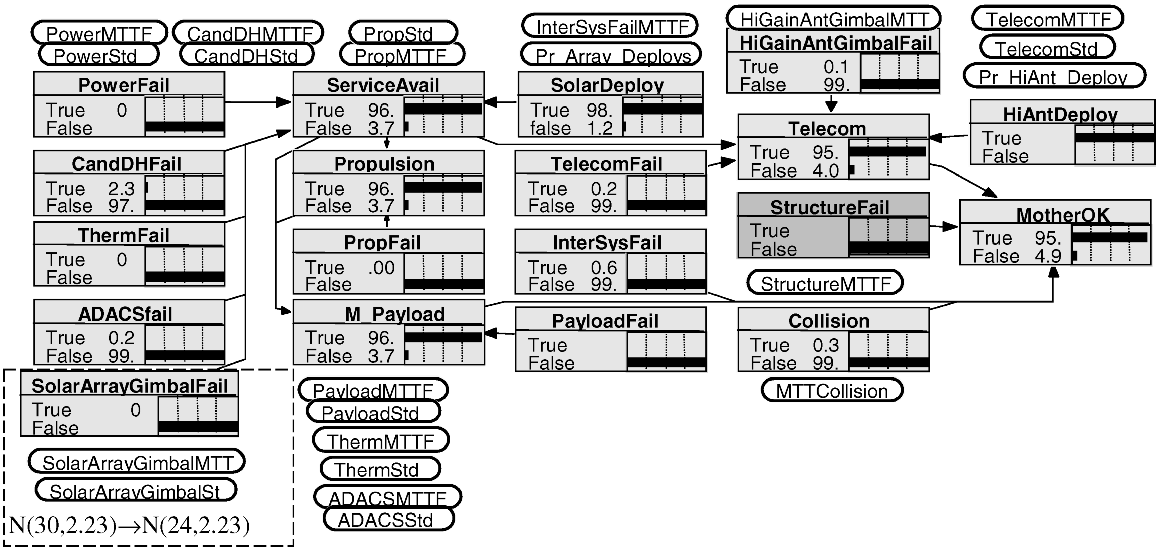

Fig. 2 Real-time what-if reliability calculations.

subsystem chair. The subsystems and mechanisms in the top two rows of Fig. 1 are grouped as a collection of basic services that are prerequisite for the proper functioning of the other subsystems. Although a failure in one such service may increase the probability of another basic service's failure, the probability distributions of initial failures in basic services were assessed by system designers as if the events were independent of one another. For example, propulsion, payload, and telecommunications can fail spontaneously but are more likely to fail if basic services are compromised. Other satellite failure modes include a breach of the structure, an unanticipated interaction among subsystems thought to be functioning correctly, or a collision with space debris.

A crucial next step in the development of this model is the assignment of probability distributions to the random variables representing the likelihood of these events. This task is tractable not only because of the small number of uncertainties, that is, the ovals in Fig. 1, but also because of the assumptions of conditional independence yield a small number of conditioning variables, that is, the number of arcs directed into each oval. For example, the basic services available node in Fig. 1 allows propulsion, telecommunications, and payload experts to assess their reliabilities as a function of the collective status of these support systems. Yet one should consider each combination of possible failures of power, command and data handling, thermal, attitude determination and control (ADAC), and solar array mechanisms contribute to the availability of basic services. The simplifying power of conditional independence would be even more apparent if subsystems were modeled including degraded as well as functioning and failed states. Additional dependencies and partial failures will need to be included in future models.[9]

The model structure and expert assessments are used to derive distributions for the survival of satellite subsystems and for the satellite as a whole, as shown in Fig 2. The ovals of Fig. 1 are replaced in Fig. 2 by bar graphs showing probabilities of satellite components' survival for 18 months or more, based on component reliability information provided by the CDE team. This display can highlight high-risk components during the CDE process. It allows quick insertion or removal of model components, for example, in Fig. 2, the probability of structural failure is set to zero, effectively removing structural risk from the model. It also permits quantified consideration of what-if scenarios. To illustrate this point, suppose that the engineer responsible for the mother satellite's mechanisms concluded that revised mission specifications would cause a solar array gimbal to be less reliable than originally believed. In Fig. 2, the probability distribution of a gimbal's lifetime in months is revised downward from a normal form of $N(\mu = 30, \sigma = 2.23)$ to $N(\mu = 24, \sigma = 2.23)$. The design team might wonder how much this would change the reliability of the satellite. The risk chair could use the model to assess quickly what impact this change would have on the chances of satellite survival. The risk chair could conclude that the change would cause the probability that the satellite remains operational for the planned mission duration to fall below 0.95 (see rows 1 and 2 of Table 1). If this impact on swarm reliability were unacceptable, the facilitator might ask another subsystem chair to improve its reliability to make up the shortfall. An automated calculation shows that the telecommunications system alone could not possibly compensate for the solar gimbal deficit (row 3 of Table 1), whereas improvement in command and data handling (C&DH) reliability could (row 4 of Table 1).

Table 1 Subsystem risk impacts satellite risk

Solar array gimbal survival, %	Telecommunications survival, %	C&DH survival, %	Satellite survival, %
99.99	99.8	97.70	95.02
99.96	99.8	97.70	94.68
99.96	100	97.70	94.90
99.96	99.8	98.04	95.01

If the satellite were in orbit and fully functional at time 0, this model could be used to assess the probability that a mother satellite operates for a hypothetical 18-month mission. The daughter model is similar to the model for the mother satellite, with daughter distinctions reflected in lifetime probability distributions and parameters assessments for the daughter satellites' components.

If the decision makers believe that too few satellites are likely to survive for the mission duration, they might switch to higher reliability components or try to include enough satellites in the swarm to make several failures tolerable.

Optimal Depth of System Decomposition

In presenting the risk status of a system to the rest of the team, the analyst may propose that combinations of more or less reliable components be used, thus, allowing the decision makers to balance risk with costs, schedule, and other attributes of their own utility functions. In between such presentations, the risk chair faces the problem of deciding to what level of detail to decompose the system for analytical purposes. Dividing a satellite into the subsystems described earlier is a natural starting point for a team consisting of such specialists. The objective of subsequent decompositions is to scrutinize high-risk components while reducing complexity by aggregating components that account for little failure risk. In practice, this would require the different subsystem chairs to have created risk models of their subsystems. Therefore, the number of alternatives to analyze may be small enough to try them all. In principle, this decomposition step could be repeated many times for a large number of design alternatives. Because computing the decision maker's utility for each alternative is not free, some preposterior estimate of the value-of-information benefits of the next decomposition level is needed to decide when to stop the decomposition efforts because of low expected returns on investment. Unfortunately, a greedy algorithm will not guarantee optimality because early choices may affect later options. In the foreseeable future, this decision should be made by the risk chair, not by the risk chair's software tools.

Satellite Launch and Dispensing

Of course, there are no guarantees that the satellites will reach orbit. Launch vehicles contribute significantly to the technical failure risk of space missions, and their performance statistics are widely available. Bayesian methods have been used to update prior distributions with each launch vehicle's track record. The resulting posterior distributions were used to estimate the probability that the vehicle chosen for the mission would be successfully launched. If the launch risks were too high, the decision maker could opt for a different vehicle or for the launch of a second vehicle in the event of an initial failure.

Even if a launch is successful, the mechanism that dispenses satellites from the launch vehicle faring presents its own risk of failure. The CDE team proposed a dispenser in which each satellite is mounted on a spindle, pressed onto a compressed spring, and held in place by one or more pins that are removed when the satellite is to be dispensed. A satellite is successfully dispensed when all its pins are removed within a short window of time. (Delayed pin removals might cause a satellite to jam on its spindle.)

To manage both the risks of premature satellite failure and dispenser failure, the decision maker might choose to include extra satellites in the swarm launch. Figure 3 contains a decision diagram modeling the uncertainties in the swarm launch. The boxes reflect choices within the decision maker's control, for example, choice of a launch vehicle and of the number of mothers and daughters in each launch vehicle. As in the satellite reliability model, the white ovals represent uncertainties outside the control of the decision maker. These decisions and uncertainties are aggregated into a single probability distribution given the number of satellites placed in orbit.

The launch and dispensing system model is combined with the earlier described mother and daughter reliability models to obtain the overall swarm reliability model shown in Fig. 4. If this combined model conjures images of rats' nests in integrated circuit or printed circuit board design, it should. Just as visualization and computational design tools have made complex electrical systems engineering manageable, complex risk assessments problems can be better analyzed with similar tools. Figure 4 shows probability computations for a hypothetical swarm launched on a single Boeing 7420-10, containing a mother and 12 daughters. Notice the probability mass distribution "NetDaughtersInSwarm" in the lower-right-hand corner of Fig. 4. The 4.06% probability for 0 daughters essentially corresponds to launch vehicle failure. The probabilities obtained for other integral numbers of daughters between 1 and 12 reflect the possibility of a successful launch and various combinations of dispensing failure. These probabilities can be used to condition the probability that the initially functioning swarm of uncertain size will survive for 18 months.

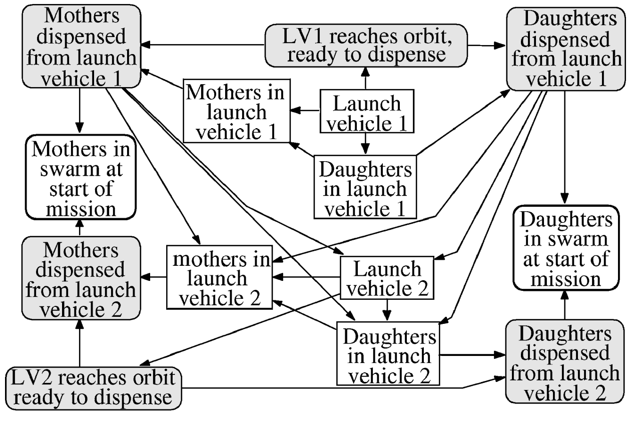
Mothers dispensed from launch vehicle 1
LV1 reaches orbit, ready to dispense
Daughters dispensed from launch vehicle 1
Mothers in launch vehicle 1
Launch vehicle 1
Mothers in swarm at start of mission
Daughters in launch vehicle 1
Daughters in swarm at start of mission
Mothers dispensed from launch vehicle 2
mothers in launch vehicle 2
Launch vehicle 2
Daughters in launch vehicle 2
Daughters dispensed from launch vehicle 2
LV2 reaches orbit ready to dispense

Fig. 3 Launch and dispensing model.

This estimate assumes that satellite failures in an operating swarm would not change the team's assessment of the failure probabilities for the remaining satellites, that is, that the satellites fail independently. Alternatively, designers could model satellite failure as dependent events whose probabilities are conditioned on the survival of other satellites in the swarm.

Swarm of Dependent Satellites

When a swarm of satellites contains many identically configured and tasked satellites, it is not surprising that they share an initial lifetime estimate. This does not imply that the lifetimes of the identical satellites are independent. On the contrary, many common causes of one satellite's failure (e.g., as a design error, an unexpectedly hostile operating environment, or a failed satellite's workload being imposed on the surviving satellites) might alter the failure risk for other satellites in the swarm given the performance of one of them. Estimates of the probabilities of these dependent failures can be incorporated into swarm reliability estimates during the design process. Even after the swarm is designed and launched, an estimate of swarm life based on dependent satellite lifetimes might be useful. The future functionality of the swarm may be an important consideration in the decision to reinforce or replace the swarm, or to schedule some activity whose success depends on reliable swarm operation. In these and other cases, decision makers might want to incorporate the history of failures within an operating swarm to update the lifetime probability distributions of remaining swarm members. A simple model of the probability of instantaneous failure of two identical, interdependent devices can be extended into a discrete-time model of the swarm lifetime that accommodates dependency in satellite lifetimes.

Dependency in a 1-of-2 Swarm: Instantaneous

Designers working with a component that is crucial to the performance of a system often include two or more identical components to improve reliability. They may assume that the redundant components fail independently. To understand the potential error when this assumption is made without justification, consider the case of a reduced swarm composed of identical daughters D_1 and D_2 as shown in Fig. 5. Suppose that, at some point in time, we are unsure whether the daughters are working or have failed. The swarm works when either or both of the two daughters are working and has failed when both daughters have failed, that is, system failure is the joint event F_1, F_2.

If the daughters are identical and their failures are independent events, $Pr\{F_1\} = Pr\{F_2\}$ and $Pr\{F_1, F_2\} = (Pr\{F_1\})^2$. However, their failures may not be independent events, and in general, the probabilities of failure of each daughter depend on whether the other has failed, even though the marginal failure probabilities $Pr\{F_1\}$ and $Pr\{F_2\}$ are equal. The joint probability of failure of two daughters can be expressed in terms of the probabilities of failure of one of them given failure or not of the other. Using the total probability theorem and the symmetries of $Pr\{F_1|\bullet\}$ and $Pr\{F_2|\bullet\}$, one obtains $Pr\{F_1, F_2\} = Pr\{F_1|F_2\} \cdot Pr\{F_1|\bar{F}_2\}/(1 - Pr\{F_1|F_2\} + Pr\{F_1|\bar{F}_2\})$. Based on this formula, Fig. 5 shows the joint probability $Pr\{F_1, F_2\}$ as a function of the probabilities of a first failure $(Pr\{F_1|\bar{F}_2\} = Pr\{F_2|\bar{F}_1\})$ and of a second failure $(Pr\{F_1|F_2\} = Pr\{F_2|F_1\})$. The intersection of that function with a parabolic sheet shows the probability that two independent daughters have both failed, that is, assuming independence so that the swarm failure probability is the square of first failure probability. Figure 5 shows how independence assumptions can 1) overstate the risk of failure for redundant dependent daughters if in fact $Pr\{F_1|F_2\} < Pr\{F_1|\bar{F}_2\}$ (corresponding, for example, to ground control actions to protect the surviving daughter, by reducing the load on a component that failed in the first daughter), or 2) understate the risk of failure if $Pr\{F_1|F_2\} > Pr\{F_1|\bar{F}_2\}$ (for example,

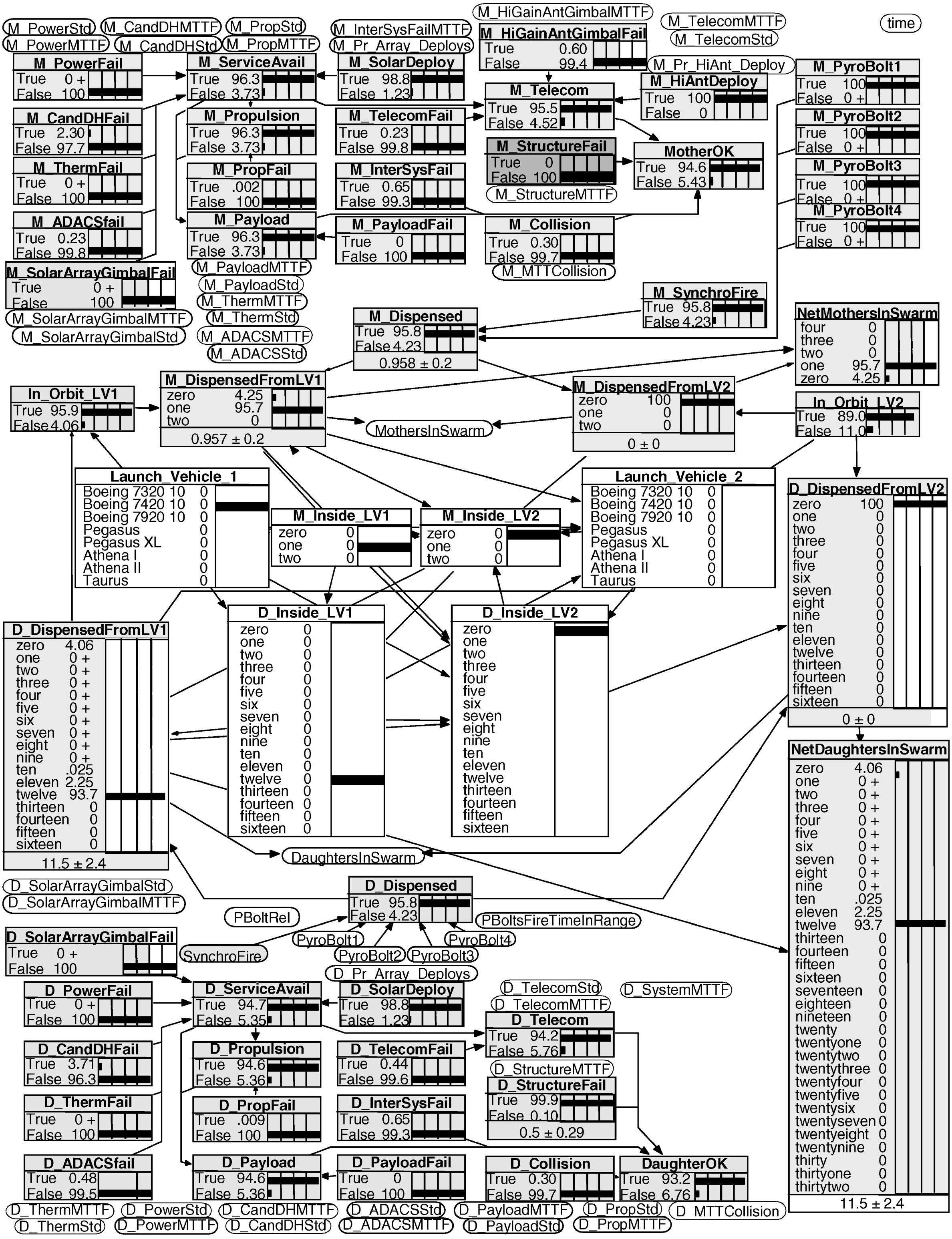

Fig. 4 Swarm reliability model (independent satellites).

when a flaw in a component installed on both daughters might be the cause of the first daughter's failure). Erroneous independence assumptions can, therefore, result in a mistaken analysis of the reliability of even simple swarms.

Dependency in a 1-of-2 Swarm: Lifetime

To assess the effect of the independence assumption on the lifetime of the two-daughter parallel swarm described earlier, consider a Markov model of the behavior of this system over a series of discrete time periods. Let p_1 be the probability of a first failure, that is, $p_1 = Pr\{X_i = 1 | X_{i-1} = 2\} = Pr\{F_2, \bar{F}_1\} + Pr\{F_1, \bar{F}_2\}$. Let p_2 be the probability of the second failure, that is, $p_2 = Pr\{X_i = 0 | X_{i-1} = 1\} = Pr\{F_2 | F_1\} = Pr\{F_1 | F_2\}$. In addition, assume that the probability that both daughters fail in the same time period is negligible and that the swarm's life begins with both daughters working, that is, $X_0 = 2$. These assumptions produce the three-state discrete Markov (death) chain shown in Fig. 6. If the two daughters fail independently, then the number of periods N before system failure is a second-order Pascal random variable with $p = p_1 = p_2$, and $Pr\{N = n\} = (n-1)p^2(1-p)^{n-2}$ and mean $\mu_N = 2/p$. If p_1

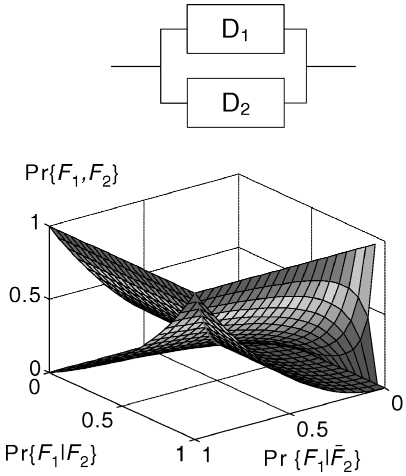

Fig. 5 Instantaneous reliability of a two-daughter system.

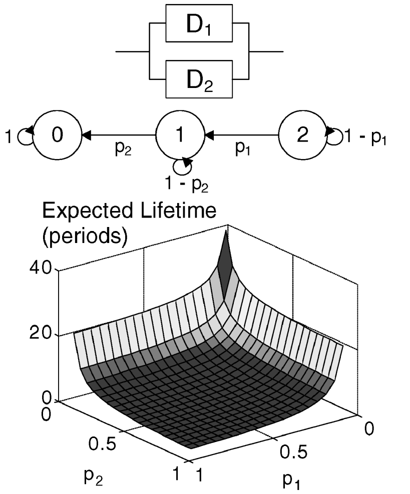

Fig. 6 Expected lifetime, two-daughter system.

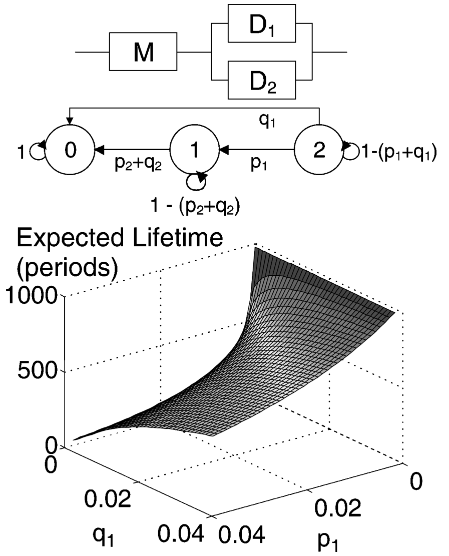

Fig. 7 Expected lifetime, mother and two-daughter system ($p_2 + q_2$ fixed at 10^{-3}).

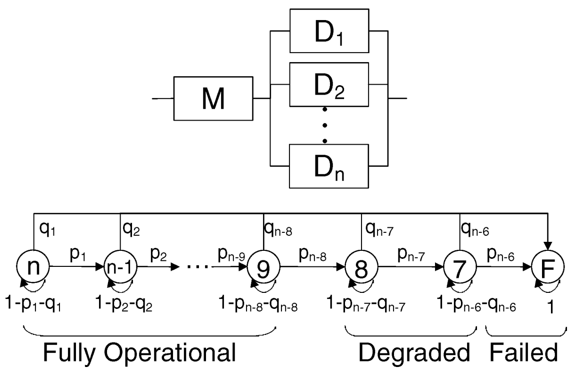

Fig. 8 Discrete-time Markov chain model for TOS reliability analysis.

differs from p_2, the expected lifetime is smaller than $2/\min\{p_1, p_2\}$; hence, the trailoff from the main diagonal in the expected lifetime graph as a function of p_1 and p_2.

Dependency in a Mother–Daughter Swarm Lifetime

Consider now a swarm that begins to resemble the architecture of the TOS study. In the slightly more complex swarm shown in Fig. 7, a mother satellite must operate in parallel with at least one of the earlier considered daughters D_1 and D_2. Retain the assumption that at most one device can fail in each period. Analysis must distinguish between a daughter failure, the first of which the swarm can survive, and the failure of the mother satellite, which causes the swarm to fail. Here p_1 and p_2 again denote daughter failures, and we now add q_i, the probability that the mother fails after $i - 1$ daughters have failed, but before the ith daughter failure. The Markov chain now has three degrees of freedom (p_1, q_1, and $p_2 + q_2$), so that the variation in swarm lifetimes can no longer be seen in a three-dimensional graph. The shape of the swarm's expected lifetime graph is much less intuitive, particularly in the high reliability part of the parameter space. The graph of expected swarm lifetime shown in Fig. 7 displays the effect of varying p_1 and q_1 while fixing $p_2 + q_2$ at 10^{-3}.

We now have the tools needed to assess the chances of survival of a swarm of satellites whose failure probabilities depend on the number of satellites that have failed previously.

Dependency in a Swarm of Satellites

The objective of the risk chair's model is to assess the probability that a launched swarm of one mother and n daughters survives a specified time period with at least seven (and preferably nine) operational daughters. By adding daughters to the Markov chain discussed earlier, we obtain the discrete-time, finite state Markov chain shown in Fig. 8 (also see Tables 2 and 3). Even if the launch is successful, the number of initially operating daughters is unknown because the success of satellite dispensing is uncertain. The reliability of the swarm shown in Fig. 8 is, therefore, conditioned on the number of functioning daughter satellites at time 0. In this discrete-time model, one period corresponds to a single orbit. A satellite orbiting the Earth at 1100 km has a period of about 105 min, so that the 18-month requirement can be translated into about 7509 orbit periods. The inner product of a vector of swarm survival probabilities conditioned on the initial swarm size being n and the vector of probabilities on values of n (Table 3) accounts for this uncertainty. We emphasize that the values for p_i and q_i shown in Table 2 are purely illustrative.

The initial-swarm failure probabilities p_1 and q_1 could be derived from the internal satellite model (such as the model in Fig. 1), but other parameters require explicit judgments of how a satellite's failure affects the expert's confidence in the survival of the remaining satellites. This judgment would hinge upon the cause of satellite failure. The premature failure of a subsystem with an extensive record of dependability, or by a collision with a fragment of space debris in an otherwise isolated orbit, might have very little impact. On the other hand, the failure of a subsystem with little or no track record might have a substantial impact on the lifetime probability distributions assigned by experts to other satellites that use the same subsystem.

Table 2 Transition probabilities

n	p_n	q_n
1	7×10^{-6}	2.2×10^{-6}
2	1.4×10^{-5}	4.4×10^{-6}
3	2.1×10^{-5}	6.6×10^{-6}
4	2.8×10^{-5}	8.8×10^{-6}
5	3.5×10^{-5}	1.1×10^{-5}
6	4.2×10^{-5}	1.32×10^{-5}
7	4.9×10^{-5}	1.54×10^{-5}
8	5.6×10^{-5}	1.76×10^{-5}
9	6.3×10^{-5}	1.98×10^{-5}
10	7×10^{-5}	2.2×10^{-5}
11	7.7×10^{-5}	2.42×10^{-5}
12	8.4×10^{-5}	2.64×10^{-5}
13	9.1×10^{-5}	2.86×10^{-5}
14	9.8×10^{-5}	3.08×10^{-5}

Table 3 TOS reliability vs number of launched daughter satellites *n*

	$Pr\{X_{7509} \geq k\}$		Expected life with k daughters (orbits)	
n	$k = 9$	$k = 7$	$k \geq 9$	$k \in \{7, 8\}$
7		0.575		13,587
8		0.836		25,866
9	0.661	0.898	18,116	19,681
10	0.888	0.918	35,523	14,974
11	0.932	0.934	54,202	11,394
12	0.950	0.950	77,473	8,669
13	0.967	0.967	113,294	6,596
14	0.983	0.983	194,898	5,019

Conclusions

This paper shows that technical failure risk assessment can be aligned with the top–down process of concurrent design engineering. Careful analysis by a risk chair, supported by integrated software tools, are needed to assess technical failure risk for a given design and how it might be improved. A top–down reliability analysis should draw on experience with each component and on expert assessments of each subsystem's lifetime. Both should be tailored to reflect how the demands of the mission will affect their lifetimes. To reduce complexity, the risk chair should focus on systems contributing significantly to the overall risk. A surprisingly useful reliability model can be constructed from a few structured probability distributions. Component reliability assessments from independent experts might be difficult for designers to obtain at this time, but some experience databases are under development.

To illustrate a risk chair's potential, this paper considered the problem of designing a satellite swarm. Without a PRA provided by a risk chair, the CDE swarm design may suffer one or more reliability penalties. First, the probability distribution of swarm performance may be unnecessarily degraded or expensive. In a critical design review, for example, an industry battery expert recommended that a redundant battery be removed to save mass. When asked how reliable the remaining battery would be, the expert responded that it was reliable enough. With a PRA model, it would have been simple to evaluate such a recommendation. Second, the analysis lays bare the impact of customer preferences on swarm technical risk. In this case, the customer's preferred launch vehicle was not reliable enough to achieve the mission reliability goals. Finally, the impact of a management policy (for example, a production strategy involving a swarm of identical daughters) on mission reliability could be quantified and influence the preliminary design.

Perhaps the most difficult challenge is the transition from risk management as performed in the current space systems design culture to a process that requires soliciting customers' risk tolerance and adapting the CDE design culture to target that risk constraint without parochial competition for resources. This requires balancing risk preferences along with the system's features, schedule, and other contributors to the customer's utility.

Choosing a stage of the design process at which to conduct a PRA presents a tradeoff between the amount of information available to support risk assessments and the effect that PRA can have on system design. CDE risk assessments are desirable and achievable, provided that customers choose to adopt an explicit, rational decision-making processes. In the meantime, so long as technical failure risk continues to be an implicit byproduct of CDE sessions, the benefits of faster and cheaper design processes must be weighed against the cost of lower-than-hoped-for reliability, or wasteful allocation of resources to achieve adequate reliability. The main theme of this paper is that this is a false choice: The model presented here shows that CDE teams can do better.

Acknowledgments

This work was supported in part by a Space Systems, Policy, and Architecture Research Consortium (SSPARC) Grant to the California Institute of Technology, the Massachusetts Institute of Technology, and Stanford University and by Grant SES-0079872 from the National Science Foundation. The authors thank their SSPARC colleagues for insights into aerospace design process and culture, Ross Shachter at Stanford and Ross Corotis at the University of Colorado for their generous discussions of the satellite influence diagram, and Sergio Guarro, William Tosney, and the failure database team at The Aerospace Corporation for discussing their ongoing research.

References

[1] Lees, F. P., *Loss Prevention in the Process Industries: Hazard Identification, Assessment, and Control*, 2nd ed., Butterworth-Heinemann, Boston, 1996, Chap. 7.

[2] *Military Handbook: Reliability Prediction of Electronic Equipment*, MIL-HDBK-217F and updates, Department of Defense, Washington DC, 1991.

[3] *Military Handbook: Electronic Reliability Design Handbook*, MIL-HDBK-338B, Department of Defense, Washington, DC, 1998.

[4] Hecht, H., and Hecht, M., "Reliability Prediction for Spacecraft," Rome Air Development Center, RADC-TR-85-229, Rome, NY, Dec. 1985.

[5] "An Early NASA Pioneer Still on the Job in Deep Space," *Space Daily* [online], 2002, SpaceDaily.com, Tokyo, Japan, URL: http://www.spacedaily.com/news/pioneer10-02c.html [cited 4 March 2002].

[6] Man, K. F., "Risk/Requirements Tradeoff Guidelines for Faster, Better, Cheaper Missions," Jet Propulsion Lab., Rept. JPL D-13277, Rev. E, California Inst. of Technology, Pasadena, CA, Feb. 1998.

[7] "Probabilistic Risk Assessment: A Bibliography," NASA Scientific and Technical Information Program, NASA SP-2000-6112, Hanover, MD, July 2000.

[8] Bourret, P., and Reggia, J. A., "A Method for Interactive Satellite Failure Diagnosis: Towards a Connectionist Solution," *Proceedings, 1989 Goddard Conference on Space Applications of Artificial Intelligence,* NASA CP-3033, NASA Technical Information Service, Washington, DC, May 1989, pp. 143–152.

[9] Loll, V. H., "Handbook in Design of Reliable Equipment," Danish Electronics, Light and Acoustics (DELTA), Rept. SPM-112, Horsholm, Denmark, Sept. 1993.

[10] Mosher, T., "Evaluating Small Satellites—Is the Risk Worth It?," *Thirteenth Annual AIAA/Utah State University Conference on Small Satellites*, Utah State Univ., Logan, UT, 1999, pp. 1–13.

[11] Howard, R. A., and Matheson, J. E. (eds.), *Readings on the Principals and Applications of Decision Analysis*, Decision Analysis, Strategic Decisions Group, Menlo Park, CA, 1983.

[12] Lowell, D. G., "Sensitivity to Relevance in Decision Analysis," Ph.D. Dissertation, Engineering Economic Systems–Operations Research, Stanford Univ., Stanford, CA, May 1994.

[13] Keeney, R. L., and von Winterfeldt, D., "On the Uses of Expert Judgment on Complex Technical Problems," *IEEE Transactions on Engineering Management,* Vol. 36, No. 2, 1989, pp. 83–86.

[14] Barlow, R. E., "Classical Statistics Is Logically Untenable," *Engineering Reliability*, ASA–SIAM Series on Statistics and Applied Probability, American Statistical Association and Society for Industrial and Applied Mathematics, Philadelphia, 1998, pp. 165–185.

[15] Hecht, H., "Reliability for Space Mission Planning," *Space Mission Analysis and Design*, edited by J. R. Wertz and W. J. Larson, 3rd ed., Department of Defense/NASA Space Technology Series, Microcosm, El Segundo, CA, 1999, pp. 765–782.

[16] Laube, R. B., "Testing of Satellites after Ground Storage," *Journal of Environmental Sciences*, Vol. 30, March–April 1987, pp. 37–41; also *Proceedings of 10th Aerospace Testing Seminar*, March 1987.

[17] Linton, D. G., "Generalized Reliability Results for 1-out-of-n:G Repairable Systems," *IEEE Transactions on Reliability,* Vol. 38, No. 4, 1989, pp. 468–471.

[18] Engel, P., "A Business of Reliability," *Sensors, Systems and Next-Generation Satellites III,* Vol. 3870, Society of Photo-Optical Instrumentation Engineers, Bellingham, WA, 1999, pp. 591–596.

[19] Frank, M. V., "Choosing Among Safety Improvement Strategies: A Discussion with Example of Risk Assessment and Multi-Criteria Decision Approaches for NASA," *Reliability Engineering and System Safety*, Vol. 49, No. 3, 1995, pp. 311–324.

[20] Murugesan, S., and Goel, P. S., "A Scheme for Fault Tolerance in Earth Sensors," *IEEE Transactions on Aerospace and Electronic Systems,* Vol. 25, No. 1, 1989, pp. 21–30.

[21] Thesker, H., and Nord, R., "High Degree of Reliability for the Cluster Satellite Fleet," *Dornier Post*, Vol. (0012-5663), No. 2, Dornier, Munich, 1994, pp. 12–13.

[22] Leveson, N. G., *Safeware: System Safety and Computers*, Addison–Wesley, Reading, MA, 1995.

[23] Paté-Cornell, M. E., and Fischbeck, P. S., "PRA as a Management Tool: Organizational Factors and Risk-Based Priorities for the Maintenance of the Tiles of the Space Shuttle Orbiter," *Reliability Engineering and System Safety*, Vol. 40, No. 3, 1993, pp. 239–257.

[24] Fragola, J. R., and McFadden, R. H., "External Maintenance Rate Prediction and Design Concepts for High Reliability and Availability on Space Station Freedom," *Reliability Engineering and System Safety*, Vol. 49, No. 3, 1995, pp. 225–273.

[25] Guarro, S. B., "The Cassini Mission Risk Assessment Framework and Application Techniques," *Reliability Engineering and System Safety*, Vol. 49, No. 3, 1995, pp. 293–302.

[26] Rasmussen, A., and Tsugawa, R., "Cost Effective Applications of Constellation Architectures of Large, Medium and Small Satellites," AIAA Paper 97-3950, Sept. 1997.

[27] Walker, R., Stokes, P. H., Wilkinson, J. E., and Swinerd, G. G., "Long-Term Collision Risk Prediction for Low Earth Orbit Satellite Constellations," *Acta Astronautica*, Vol. 47, No. 2–9, 2000, pp. 707–717; also International Academy of Astronautics, IAA Paper 99-6604, Oct. 1999.

[28] Paté-Cornell, M. E., and Sachon, M., "Risks of Particle Hits during Space Walks in Low Earth Orbit," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 40, No. 3, 2001, pp. 134–146.

[29] Guikema, S. D., and Paté-Cornell, M. E., "The Danger of Myopic Conservation in Risk Analysis: The Problem of Time Allocation for the Deep Space Network," AIAA Paper 2001-4518, Aug. 2001.

[30] Guikema, S. D., and Paté-Cornell, M. E., "Component Choice for Managing Risk in Engineered Systems with Generalized Risk/Cost Functions," *Reliability Engineering and System Safety*, Vol. 78, No. 3, 2002, pp. 227–238.

[31] Walton, M., and Hastings, D., "Quantifying Embedded Uncertainty of Space Systems Architectures in Conceptual Design," AIAA Paper 2001-4573, Aug. 2001.

[32] Thaggard, M., "Databases for Reliability and Probabilistic Risk Assessment," *Annual Reliability and Maintainability Symposium,* Inst. of Electrical and Electronic Engineers, New York, 1995, pp. 327–336.

[33] Helgevold, D. P., and Crosse, L. P., "Interim Results of an On-orbit Anomaly Study," 17th Aerospace Testing Seminar, Inst. of Environmental Sciences, Oct. 1997, pp. 325–331; also Paper A98-33265 08-14, Oct 1997.

[34] Lee, S.-H., Boeck, M. L., Pfau, B. L., Quintero, A. H., Steffan, K. F., Tosney, W. F., and Wong, B., "System Specification for the Space Systems Engineering Database (SSED)," The Aerospace Corporation, Rept. TOR-99(5457)-6, El Segundo, CA, 1999.

[35] Neogy, R., and Siu, C.-P., "A Satellite Failure Database System," *Annual Reliability and Maintainability Symposium*, Inst. of Electrical and Electronics Engineers, New York, 1988, pp. 422–425.

[36] Hoffman, D. R., "An Overview of Concurrent Engineering," *Annual Reliability and Maintainability Symposium,* Inst. for Electrical and Electronic Engineers, New York, 1998, pp. 1–7.

[37] Guarro, S. B., "Guest Editorial," *Reliability Engineering and System Safety*, Vol. 49, No. 3, 1995, pp. 213–216.

[38] Dillon, R. L., Paté-Cornell, M. E., and Guikema, S. D., "Programmatic Risk Analysis for Critical Engineering Systems Under Tight Resource Constraints," *Operations Research*, Vol. 51, No. 3, 2003, pp. 354–370.

[39] McManus, H. L., and Warmkessel, J. M., "Creating Advanced Architectures for Space Systems: Emergent Lessons from New Processes," *Journal of Spacecraft and Rockets*, Vol. 41, No. 1, 2004, pp. 69–74.

J. Korte
Guest Editor