Second International Symposium on Engineering Systems
MIT, Cambridge, Massachusetts, June 15-17, 2009

Design for Survivability:
Concept Generation and Evaluation in Dynamic Tradespace Exploration

M.G. Richards,[1] D.E. Hastings,[2] D.H. Rhodes,[3] A.M. Ross,[4] and A.L. Weigel[5]
Massachusetts Institute of Technology, Cambridge, MA, 02139

Multi-Attribute Tradespace Exploration (MATE) for Survivability is introduced as a system analysis methodology to improve the generation and evaluation of survivable alternatives during conceptual design. MATE for Survivability applies decision theory to the parametric modeling of thousands of design alternatives across representative distributions of disturbance environments. To improve the generation of survivable alternatives, seventeen empirically-validated survivability design principles are introduced. The general set of design principles allows the consideration of structural and behavioral strategies for mitigating the impact of disturbances over the lifecycle of a given encounter. To improve the evaluation of survivability, value-based metrics are introduced for the assessment of survivability as a dynamic, continuous, and path-dependent system property. Finally, the survivability "tear(drop)" tradespace is introduced to enable the identification of inherently survivable architectures that efficiently balance performance metrics of cost, utility, and survivability. The internal validity and prescriptive value of the design principles, metrics, and tradespaces comprising MATE for Survivability are established through applications to the designs of an orbital transfer vehicle and a satellite radar system.

Key words: survivability, tradespace exploration, system architecture, engineering systems

1. Introduction

The operational environment of engineering systems is increasingly characterized by disturbances which may asymmetrically degrade performance, particularly for interdependent infrastructure systems. In recent years, hostile actors have preyed upon infrastructures which may be linked, whether physically, electrically, or economically.[1] Engineering systems are also vulnerable to non-intelligent threats arising from the natural environment.[2,3] In response to these

---

[1] Ph.D. Graduate, Engineering Systems Division (ESD), mgr@alum.mit.edu.
[2] Professor, Department of Aeronautics and Astronautics and ESD, hastings@mit.edu.
[3] Senior Lecturer, ESD, rhodes@mit.edu.
[4] Research Scientist, ESD, adamross@mit.edu.
[5] Assistant Professor, Department of Aeronautics and Astronautics and ESD, alweigel@mit.edu.

synthetic and natural disturbances, numerous studies and several government and academic research initiatives have been launched.[4,5,6,7] While related in terms of the common objective of protecting critical societal infrastructure, traditional approaches towards mitigating disturbances have evolved almost exclusively within the context of individual engineering disciplines and infrastructure domains.

Survivability engineering is the subset of systems engineering concerned with minimizing the impact of environmental disturbances on system performance. Survivability may be defined as the ability of a system to minimize the impact of a finite-duration disturbance on value delivery (*i.e.*, stakeholder benefit at cost), achieved through (1) the reduction of the likelihood or magnitude of a disturbance, (2) the satisfaction of a minimally acceptable level of value delivery during and after a disturbance, and/or (3) a timely recovery.[8]

This paper introduces a system analysis methodology for incorporating survivability considerations into the conceptual design of engineering systems. Following the problem statement and research questions (Section 2), an operational definition of survivability is introduced (Section 3). To improve concept generation, a set of seventeen empirically-validated survivability design principles is introduced for expanding the set of system design trade-offs under consideration (Section 4). To improve concept evaluation, value-based survivability metrics are introduced to incorporate survivability considerations into tradespace exploration (Section 5). Finally, Multi-Attribute Tradespace Exploration (MATE) for Survivability is introduced as an end-to-end methodology for system analysts to apply the survivability design principles and metrics during conceptual design (Section 6). The paper concludes with a brief note on the contribution of this research to systems architecting (Section 7).

2. Problem Formulation

2.A. Problem Statement

In addition to meeting requirements in a static context, the performance of engineering systems is increasingly defined by an ability to deliver value to stakeholders in the presence of changing operational environments, economic markets, and technological developments.[9] As temporal system properties that reflect the degree to which systems are able to maintain or even improve function in the presence of change, the "ilities" (*e.g.*, flexibility) constitute a rich area of research for improving value delivery over the lifecycle of systems.[10] Applicable across engineering domains, the "ilities" are particularly critical to aerospace systems which are characterized by high cost, long design lives, high complexity, interdependencies with other systems, and dynamic operational contexts.[11]

Although survivability is an emergent system property that arises from interactions among system components and between a system and its environment, conventional approaches to survivability engineering are often reductionist in nature (*i.e.*, focused only on selected properties of subsystems or modules in isolation).[12] Furthermore, existing survivability engineering methodologies are normally based on specific operating scenarios and presupposed disturbances rather than a general theory with indeterminate threats. As a result, current methods neither accommodate dynamic threat environments nor facilitate stakeholder communication for trading among system lifecycle cost, performance, and survivability

Given the limitations of existing survivability design methods for aerospace systems (*i.e.*, treatment of survivability as a constraint on design, static system threat assessment reports, assumption of independent weapon encounters, limited scope, and exclusive focus on physical integrity),[13] there is a need for a design method that (1) incorporates survivability as an active trade in the design process, (2) captures the dynamics of operational environments over the entire lifecycle of systems, (3) captures path dependencies of system survivability to disturbances, (4) extends in scope to architecture-level survivability assessments, and (5) takes a value-centric perspective to allow alternative value-delivery mechanisms in the tradespace. Recent research on how decision-makers can recognize and evaluate dynamically relevant designs, including Multi-Attribute Tradespace Exploration[14] and Epoch-Era Analysis[15], offers a theoretical foundation for the development of an improved design methodology for survivability.

2.B. Research Questions

The following research questions are posed to address the survivability analysis challenges identified in the preceding problem statement.

1. What is a dynamic, operational, and value-centric definition of survivability for engineering systems?
2. What design principles enable survivability?
3. How can survivability be quantified and used as a decision metric in exploring tradespaces during conceptual design of aerospace systems?
4. For a given space mission, how can alternative system architectures in dynamic disturbance environments be evaluated in terms of survivability?

The first research question aims to conceptualize and operationalize survivability for subsequent investigation. A general definition of survivability is a critical first step because existing metrics for survivability vary among domains and are traditionally calculated with specific operational scenarios in mind. The goal of the second question is to develop a framework of structural and behavioral principles that enable survivability across the entire lifecycle of disturbances. The principles are to provide designers with a portfolio of concept-neutral strategies for achieving survivability during concept generation. Existing sets of survivability design principles tend to exclude non-physical factors and to focus on concept-specific techniques. The third question identifies the core challenge of the proposed research: quantification of a particular "ility" to enable its specification, evaluation, and verification during the conceptual design of aerospace systems. Despite the general agreement regarding the importance of the "ilities", they are neither well-defined nor easily evaluated in isolation. Finally, the purpose of the fourth question is to apply the theories and methods developed in answering the previous questions to current design issues in space system architecture. In particular, emerging military space radar concepts will evaluated across threat environments. Addressing this question is of vital importance to the U.S., given the tens of billions of dollars at stake and the cyclical establishment and cancellation of space radar programs over the past decade.[16]

3. Definition of Survivability

The first research question aims to conceptualize and operationalize survivability for subsequent tradespace exploration. Survivability may be defined in physical terms as "the capability of a system to avoid or withstand hostile natural and manmade environments without suffering abortive impairment of its ability to accomplish its designated mission.”[17] Survivability may also be defined, more generally, as *the ability of a system to minimize the impact of finite-duration environmental disturbances on value delivery*. A value-centric definition of survivability is desirable during conceptual design because it provides a fundamental metric for relating system properties to desired stakeholder outcomes. Taking the value-centric perspective empowers decision-makers to compare technically dissimilar system concepts using a unifying set of attributes. The ability to consider multiple system concepts is particularly useful for survivability when original value delivery mechanisms may be blocked by a disturbance.

In defining survivability, it is also important to recognize its inherently dynamic nature. Survivability emerges from the interaction of a system with its environment over time. Depending on stakeholder needs, survivability requirements may allow limited periods during which the system operates in a degraded state, unavailable state, or safe mode. Recognizing survivability as a dynamic system property informs three general survivability design strategies over the lifecycle of a disturbance. Type I survivability, *susceptibility reduction*, is the reduction of the likelihood of or magnitude of a disturbance. Type II survivability, *vulnerability reduction*, is the minimization of the disturbance-induced losses on value delivery. (Systems that are Type II-survivable may exhibit graceful degradation in which at least minimal functionality is maintained in the event of disturbance-induced losses. The reduced magnitude and rate of value losses in systems that degrade gracefully contrasts with fragile systems where small disturbances may cause total system failure.) Type III survivability, *resilience enhancement*, is the maximization of the recovery of value-delivery within a permitted recovery time.

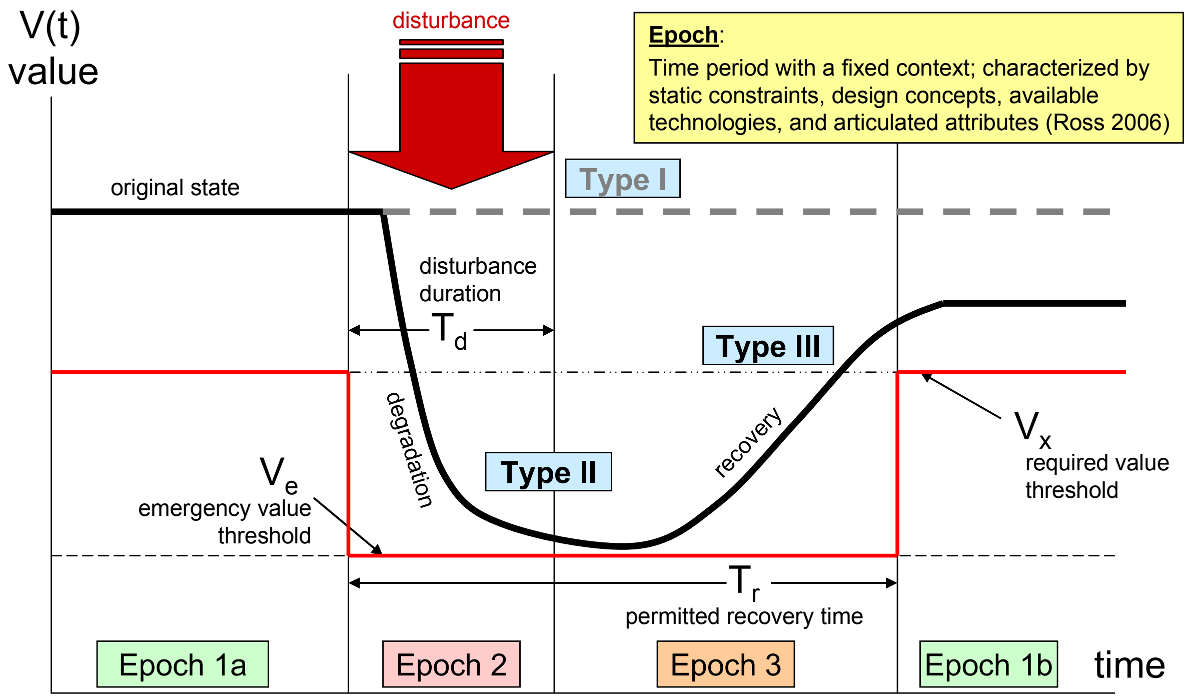

Figure 1. Conceptualization of Survivability

Figure 1 provides a notional illustration of Type I, Type II, and Type III survivability in terms of value delivery over time [$V(t)$]. Time is discretized across four epochs, periods of a fixed context with static stakeholder needs. Following successful value delivery during baseline environmental conditions and stakeholder expectations (Epoch 1a), the system experiences a finite disturbance that degrades performance. Value delivery expectations on the system may be lower during the disturbance (Epoch 2) and in the time period immediately following (Epoch 3) before returning to baseline expectations (Epoch 1b). Type I survivability, depicted as a dashed horizontal line, is achieved if the disturbance fails to reduce $V(t)$ below the required value threshold [V_x] over all of the epochs. In order to determine whether the system is Type II or Type III survivable, two additional factors must be defined: the minimum acceptable value to be delivered during and immediately after the disturbance [V_e] and the permitted recovery time elapsed past the onset of the disturbance [T_r]. In Figure 1, the solid line depicts a system achieving Type II survivability by maintaining $V(t)$ at a level above V_e during Epoch 2 and Epoch 3. The solid line also depicts a Type III-survivable system as $V(t)$ recovers to a level above V_x within T_r.

4. Survivability Design Principles

The goal of the second research question is to develop a framework of structural and behavioral principles that enable survivability across the entire lifecycle of disturbances. The principles provide designers with a portfolio of concept-neutral strategies of architectural choice for achieving survivability during concept generation. Existing sets of survivability design principles tend to exclude non-physical factors and to focus on concept-specific techniques. A general set of design principles allows the consideration of survivability strategies that may mitigate disturbances across the entire lifecycle of a given encounter. Within the context of tradespace exploration, the design principles are intended to augment the creativity of system designers by ensuring evaluation of a broad set of design alternatives.

Seventeen empirically-validated survivability design principles were identified in an iterative process of hypothesis generation and testing. Twelve design principles for enhancing survivability were initially deduced from a generic system-disturbance representation, from consulting the literature, and from retrospective case studies (*e.g.*, U.S. nuclear command and control system during the Cold War). Next, the validity of these initial results were tested by inductively mapping the survivability features of the A-10 Thunderbolt II combat aircraft and of the UH-60A Blackhawk helicopter to the design principle set.[18] Results from this mapping identified missing design principles, taxonomic imprecision in design principle definitions, and deficiencies in the underlying system-disturbance framework—requiring an expansion to a set of seventeen design principles. Subsequent empirical testing validated the completeness of the seventeen design principles when applied to the Iridium satellite communications system and the F-16C Fighting Falcon.[19] Table 1 shows the seventeen design principles, spanning Type I, Type II, and Type III survivability strategies.

Table 1. Validated Set of Survivability Design Principles

Type I (Reduce Susceptibility)		
1.1	prevention	suppression of a future or potential future disturbance
1.2	mobility	relocation to avoid detection by an external change agent
1.3	concealment	reduction of the visibility of a system from an external change agent
1.4	deterrence	dissuasion of a rational external change agent from committing a disturbance
1.5	preemption	suppression of an imminent disturbance
1.6	avoidance	maneuverability away from an ongoing disturbance
Type II (Reduce Vulnerability)		
2.1	hardness	resistance of a system to deformation
2.2	redundancy	duplication of critical system functions to increase reliability
2.3	margin	allowance of extra capability for maintaining value delivery despite losses
2.4	heterogeneity	variation in system elements to mitigate homogeneous disturbances
2.5	distribution	separation of critical system elements to mitigate local disturbances
2.6	failure mode reduction	elimination of system hazards through intrinsic design: substitution, simplification, decoupling, and reduction of hazardous materials
2.7	fail-safe	prevention or delay of degradation via physics of incipient failure
2.8	evolution	alteration of system elements to reduce disturbance effectiveness
2.9	containment	isolation or minimization of the propagation of failure
Type III (Enhance Resilience)		
3.1	replacement	substitution of system elements to improve value delivery
3.2	repair	restoration of system to improve value delivery

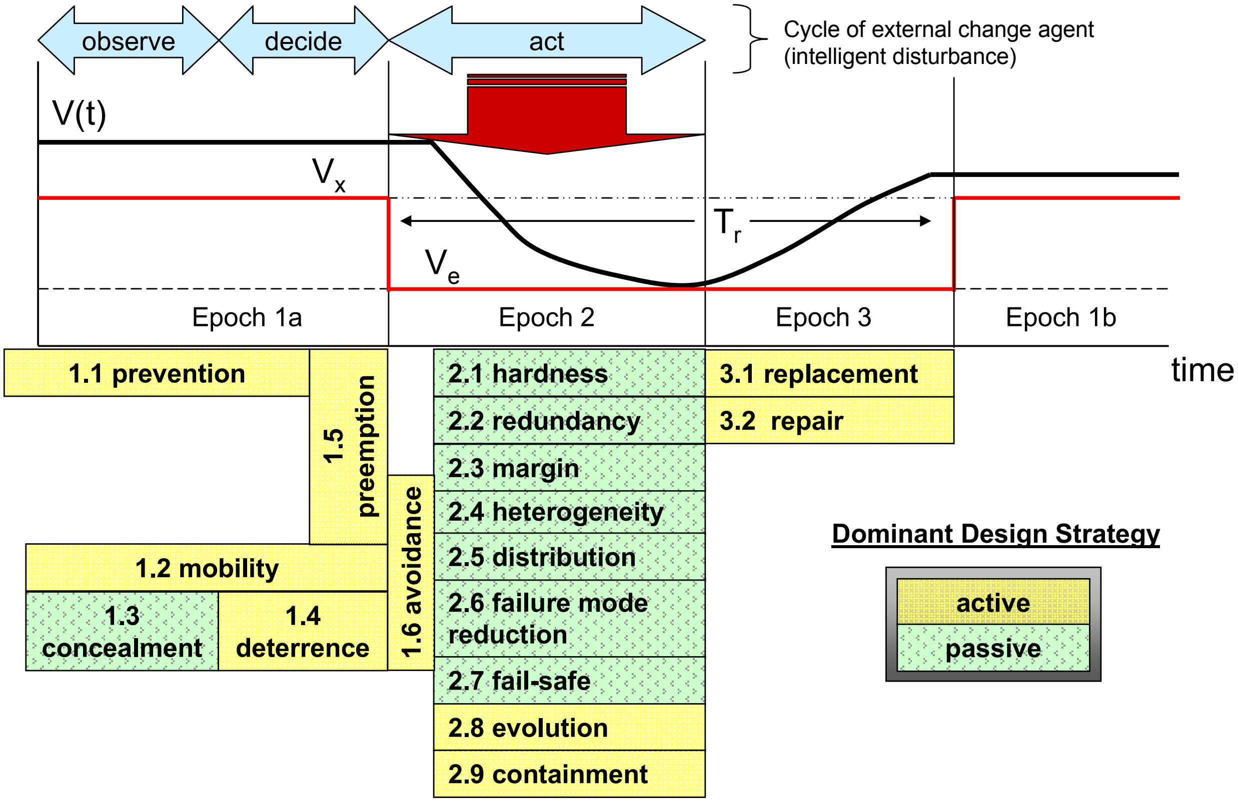

Figure 2. Mapping of Design Principles to Disturbance Lifecycle

Figure 2 depicts the time intervals during which each of the seventeen design principles may positively affect value delivery in a disturbance lifecycle. Each design principle is classified as either passive or active. A focus on passive principles will lead to the construction of closed (static) systems that resist disturbance based on projections of the operational environment. A focus on active principles will lead to the construction of open (dynamic) systems that cope with future uncertainty by stressing architectural agility to recover from disturbances. The distinction between passive and active survivability is useful because it specifies which design principles may be used based on the changeability of the architecture. As demonstrated in a MATE for Survivability study of a satellite radar system,[20] the design principles may be consulted both to augment the creativity of system designers by ensuring consideration of a broad set of design alternatives and to quickly screen a large number of candidate design variables before proceeding to concept evaluation.

5. Survivability Metrics

Survivability is evaluated based on the relationship between stochastic trajectories of system value delivery (*e.g.*, multi-attribute utility over time) and critical value thresholds elicited from a decision-maker (*i.e.*, required value threshold, emergency value threshold, and permitted recovery time).[21] For example, Figure 3 shows a sample utility trajectory and set of critical value thresholds for an orbital transfer vehicle. The ten-year operational life is characterized by a series of non-catastrophic debris impacts and two restorative servicing operations.

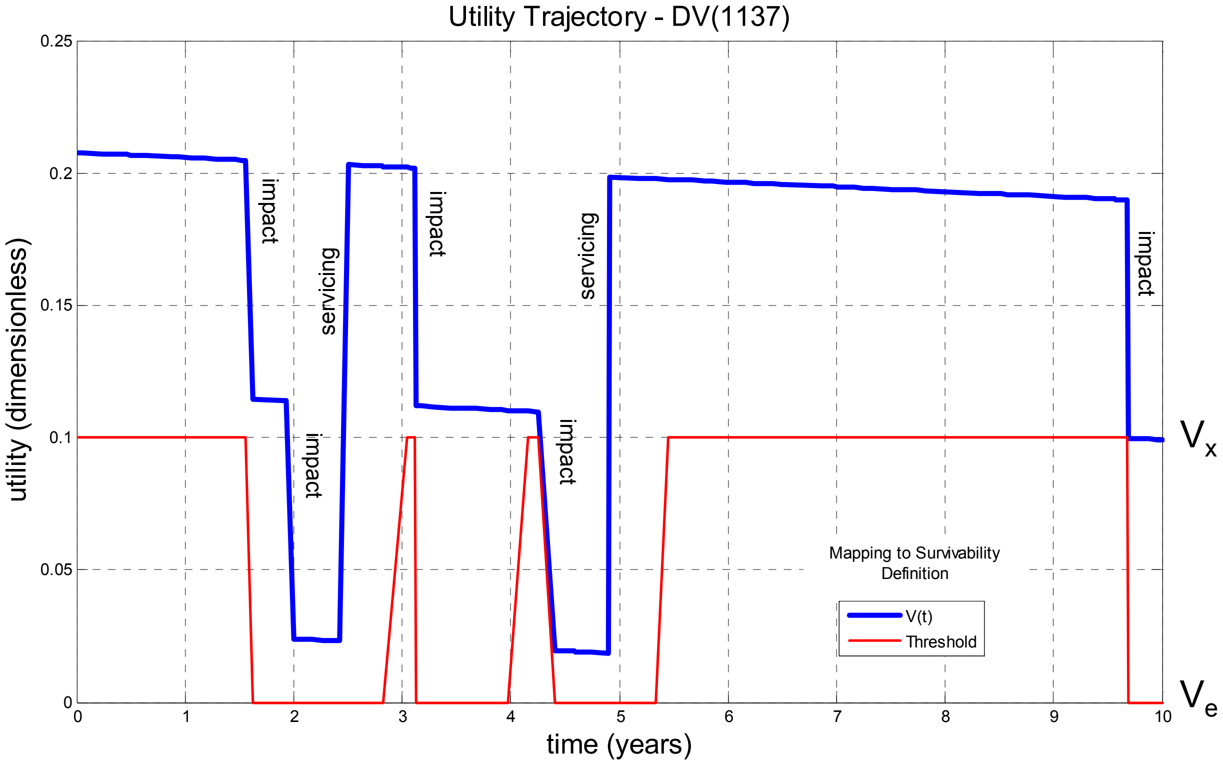

Figure 3. Sample Utility Trajectory

The characterization of system value delivery provided by the utility trajectories allows survivability to be evaluated as a dynamic, continuous, and path-dependent system property. In particular, two metrics are proposed to summarize the relationship between utility trajectories and critical value thresholds: *time-weighted average utility loss* and *threshold availability*. In keeping with the survivability definition, these metrics collectively evaluate the ability of a system to minimize value losses while meeting critical value thresholds before, during, and after environmental disturbances.

Time-weighted average utility loss assesses the difference between the design utility (at beginning-of-life), U_o, and the time-weighted average utility achieved over the system design life, T_{dl}:

$$\overline{U}_L = U_0 - \frac{1}{T_{dl}} \cdot \int U(t)\ dt$$

While time-weighted average utility loss is useful for evaluating the impact of various survivability features on a single system, it is less useful for comparisons across systems since U_o is not conserved across designs. Therefore, to appreciate the survivability implications of a system's ability both to incorporate margin in value delivery and to minimize losses in value, it is necessary to evaluate time-weighted average utility loss from the design utility value, U_o.

Threshold availability assesses the ability of a system to meet critical value thresholds. Specifically, it is defined as the ratio of the time that $U(t)$ is above operable (required or emergency) utility thresholds (*i.e.*, time above thresholds [TAT]) to the total design life:

$$A_T = \frac{TAT}{T_{dl}}$$

As survivability is a stochastic, path-dependent property, a single utility trajectory from a single design alternative is not necessarily representative or meaningful from a decision-making perspective. Rather, each utility trajectory constitutes one data sample from a continuous distribution of potential system lifecycles. For example, Figure 4 depicts six more sample utility trajectories from two alternative orbital transfer vehicles: design vectors 19 and 1137 (top and bottom rows, respectively).

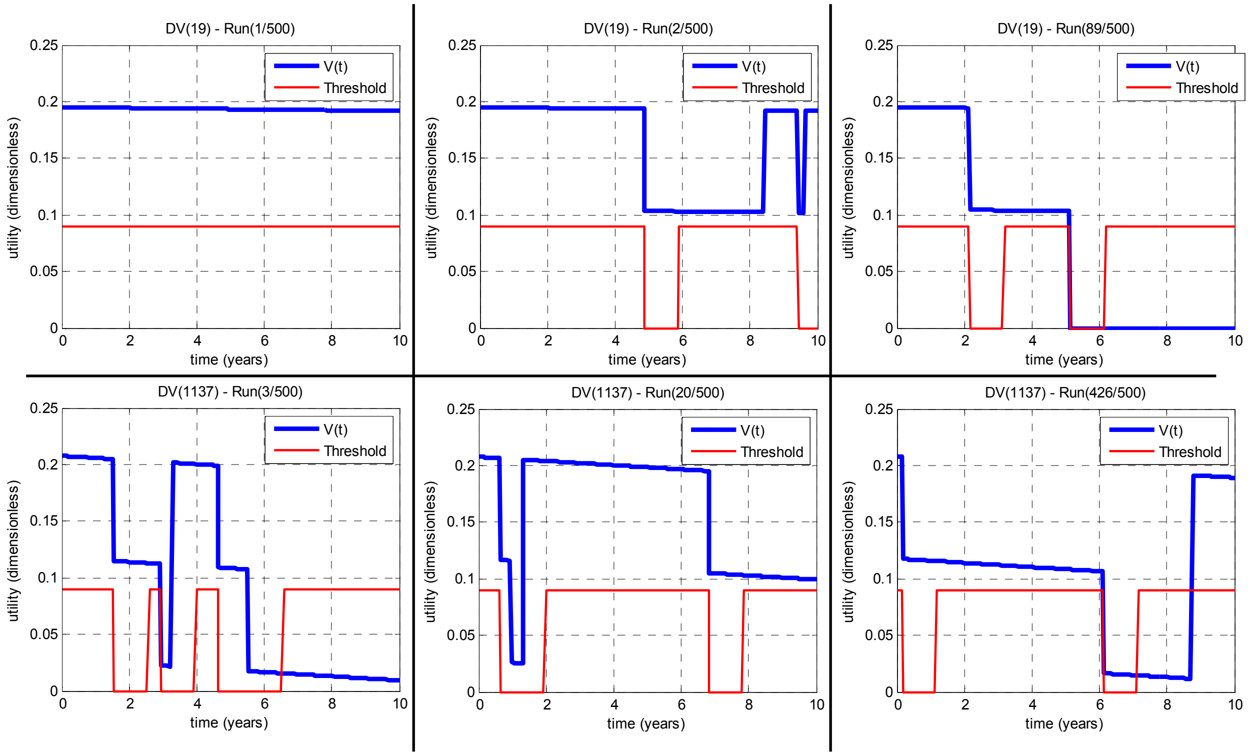

Figure 4. Need for Summary Statistics across Simulation Runs

In addition to summarizing the performance of one design alternative across Monte Carlo trials, there is a need to distinguish among different design alternatives in the tradespace. However, observing all of the utility trajectories generated in a MATE for Survivability study—typically 500 or more for each of several thousand design alternatives—is not practical. Therefore, time-weighted average utility loss and threshold availability are applied as aggregate measures for each set of utility trajectories.

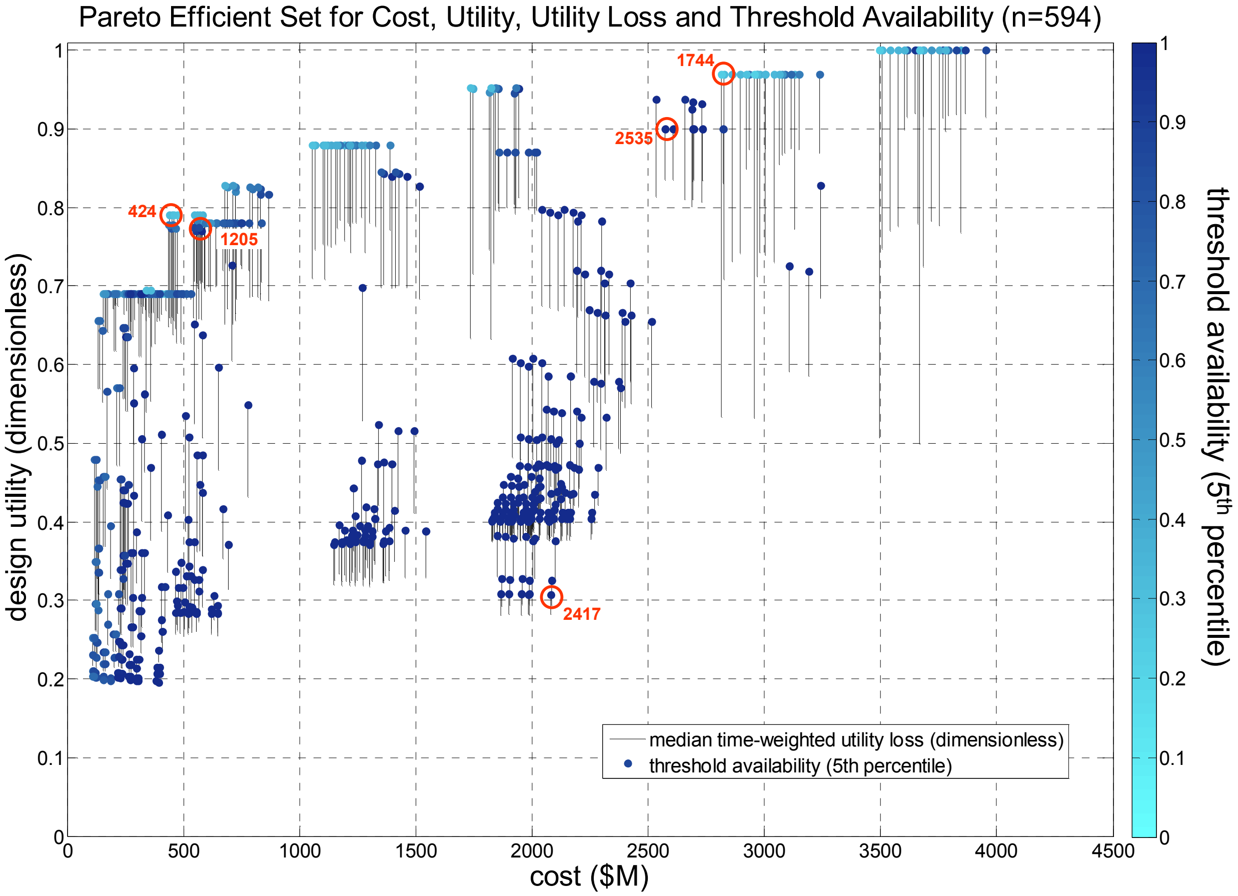

Figure 5. Four-Dimensional Pareto Surface of Survivability Tear Tradespace

Figure 5 shows how the survivability metrics may be integrated with traditional performance metrics of cost and utility in a survivability "tear(drop)" tradespace. The survivability tear tradespace provides a new approach for conducting survivability trades during conceptual design by integrating survivability considerations into the selection of the baseline system concept. (Use of the word "tear" is meant to describe regret associated with system utility loss.) The survivability tear tradespace preserves the axes in a traditional MATE analysis by plotting alternative system designs in terms of cost and utility. The new probabilistic survivability metrics are integrated using shade for threshold availability (5^{th} percentile) and a line drawn between utility and (median) time-weighted average utility to indicate (median) time-weighted utility loss. As illustrated in Figure 5, the large number of designs in the survivability tear tradespace may be filtered over the four-dimensional Pareto surface of cost, utility, time-weighted average utility loss, and threshold availability. This expanded region of Pareto efficiency reveals several interesting designs in the interior of the tradespace. While not located along the Pareto front of cost and utility, these designs join the "optimal" set based on performance in the survivability metrics.

6. Multi-Attribute Tradespace Exploration (MATE) for Survivability

Multi-Attribute Tradespace Exploration for Survivability is a general methodology for the assessment of alternative system architectures that must operate in dynamic disturbance environments.[22] In particular, the existing MATE process (*i.e.*, a solution-generating and decision-making framework that applies decision theory to model-based design)[14] is extended to leverage the proposed survivability design principles and metrics in concept generation and concept evaluation, respectively. MATE for Survivability consists of eight iterative phases: (1) define system value proposition, (2) generate concepts, (3) specify disturbances, (4) apply survivability principles, (5) model baseline system performance, (6) model impact of disturbances on dynamic system performance, (7) apply survivability metrics, and (8) select designs for further analysis. Figure 6 provides a flow chart of the process and identifies relationships with the legacy MATE process.

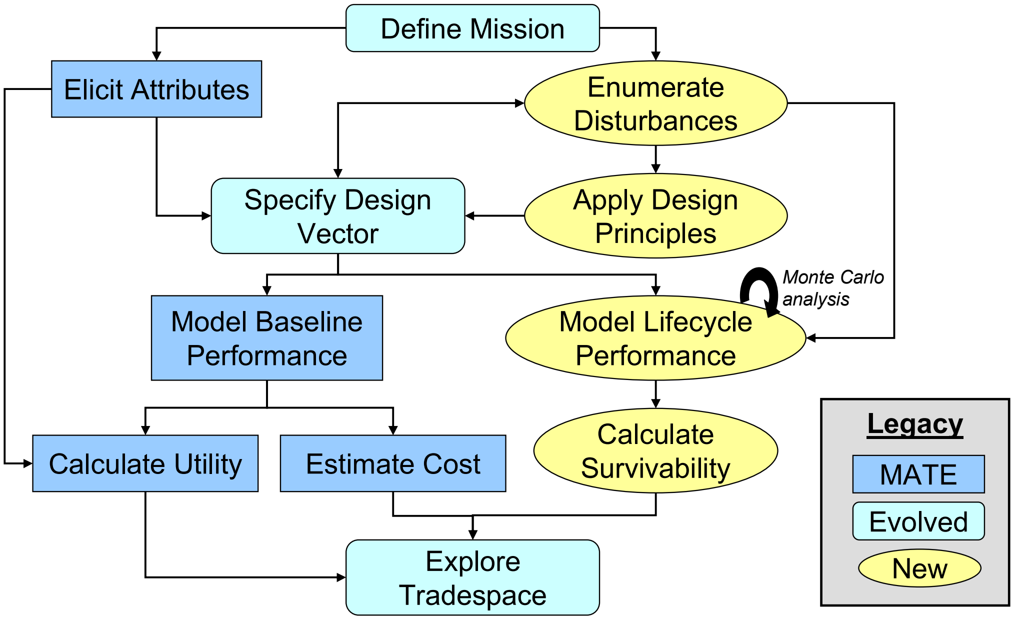

Figure 6. Multi-Attribute Tradespace Exploration (MATE) for Survivability

A satellite radar case application[23] demonstrates the prescriptive insights that may be yielded from a MATE for Survivability analysis. Thousands of architectural alternatives are evaluated for a future military satellite radar capability, including various satellite designs, constellation structures, and supporting communications networks.

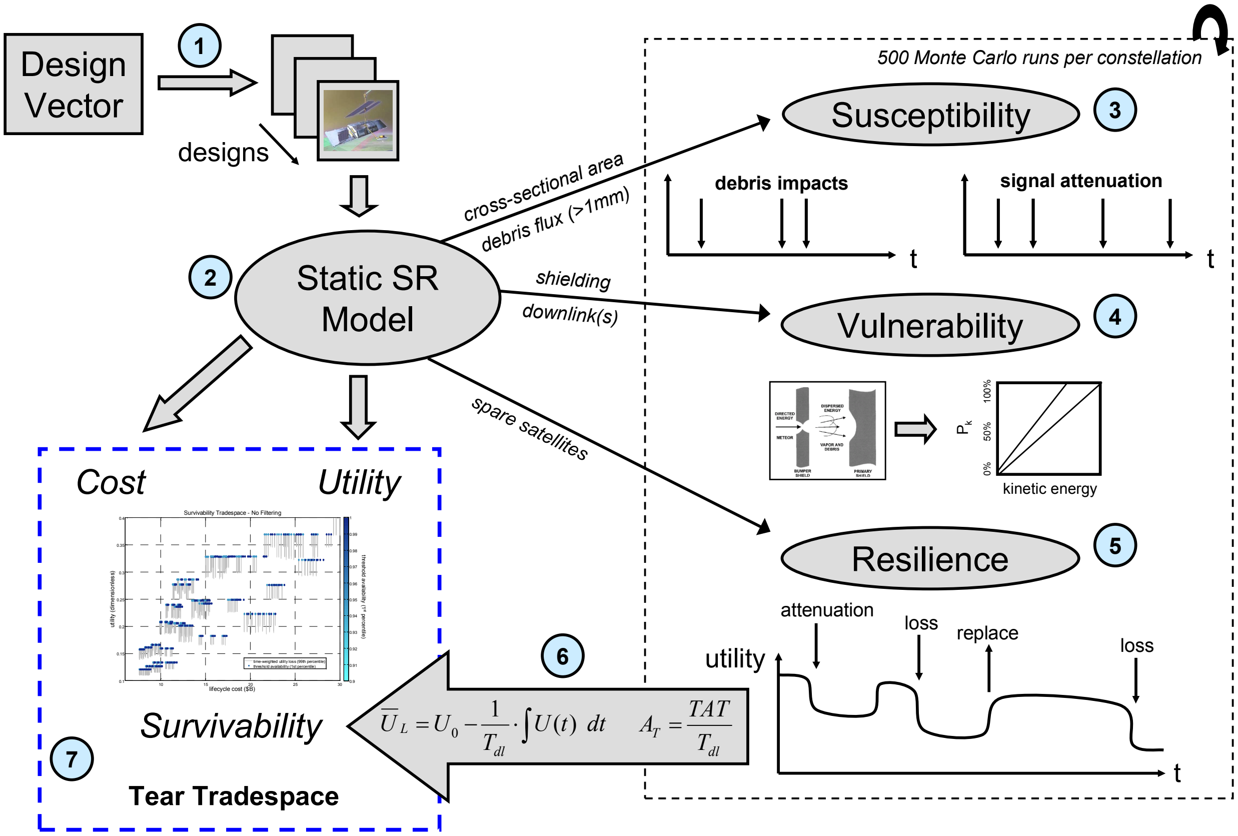

Figure 7. Incorporation of Survivability Considerations into Satellite Radar Tradespace

Figure 7 provides a flow-chart representation of how survivability considerations are incorporated into the satellite radar tradespace by modeling lifecycle performance. Treating the static tradespace model as a black-box, implementation of the survivability analysis involves seven general steps. (These seven steps outline lifecycle performance modeling activities, and are not to be confused with the eight phases comprising MATE for Survivability.) First, the design vector is expanded to include survivability design variables. Second, a physics-based model of satellite radar performance is used to assess the total lifecycle cost and design utility of 3,888 design alternatives. Third, susceptibility to debris impacts is modeled as a function of the exposed cross-sectional area of alternative constellations and debris flux. Fourth, the vulnerability of the designs to debris and signal attenuation is calculated as a function of satellite shielding and available communications downlinks. Fifth, the resilience of each design is assessed based on the availability of satellite spares. By continuously monitoring constellation performance in the attributes, multi-attribute utility is assessed over the entire lifecycle. Sixth, time-weighted average utility loss and threshold availability are calculated at the end of each ten-year simulation as summary statistics for the utility trajectory output. As each run of the simulation is stochastic and path-dependent, a 500-run Monte Carlo analysis is performed for each design to obtain a representative distribution of utility trajectories. Seventh, the probabilistic survivability metrics are integrated with the deterministic metrics of lifecycle cost and design utility for integrated tradespace exploration.

Many lessons are extracted from the satellite radar case application. Most fundamentally, the model results indicate that the satellite radar alternatives within the design vector are survivable to the space environment. However, the tear tradespace analysis shows that the rank-order preferences of the decision-maker on alternatives are subject to change when threats are taken into account. Response surface plots also yielded several insights regarding the impact of alternative survivability design variables. In particular, shielding is found to have a small impact on time-weighted average utility, while communications redundancy is very important for maintaining threshold availability. Investments in satellite spares have a variable impact, with sparse constellations benefitting the most from the option to rapidly reconstitute. Interestingly, survivable designs that are most insensitive to decision-maker risk preferences are found to mitigate disturbances architecturally. By using the tear tradespace, constellations are identified that have similar cost and utility but with variable survivability performance. By sacrificing individual satellite performance and accepting moderate growth in lifecycle cost through selecting a more distributed constellation of less-capable satellites, it is possible to achieve higher levels of survivability.

The application of MATE for Survivability to satellite radar also demonstrates the advantages of the methodology relative to existing approaches. As with the orbital transfer vehicle computer experiment, the analysis of satellite radar shows that using tradespace exploration solely to identify designs on the traditional Pareto front of cost and utility excludes the most survivable designs. Furthermore, the methodology allows system-level and architecture-level survivability trades to be made in concert rather than delaying survivability considerations until after selection of a baseline system concept. As demonstrated by the response surfaces for the survivability design variables,[23] incorporating survivability considerations into the definition of the system concept is important if the dedicated survivability design variables (*e.g.*, shielding) are less critical to achieving survivability than the fundamental system architecture (*e.g.*, constellation type). By applying the concept-neutral criteria of lifecycle cost, multi-attribute utility, and the survivability metrics, the tear tradespaces may be used to identify promising design alternatives among thousands of technically-diverse systems.

7. Conclusion

MATE for Survivability seeks to address the motivation outlined in the problem statement by enhancing the generation and evaluation of design alternatives that maintain value delivery in the presence of finite-duration disturbances. While existing survivability engineering techniques optimize the physical survivability of individual systems, the evolution of engineering systems to higher levels of complexity necessitates architectural solutions to emerging threats. Accordingly, MATE for Survivability complements existing survivability approaches focused on detailed design trades by allowing survivability considerations to be incorporated into the selection of the baseline architectural concept. It is hoped that the survivability design principles and metrics may be applied prescriptively as analytic tools, shifting one aspect of the systems architecting process from an art to a science.

Acknowledgements

Funding for this work was provided by the Systems Engineering Advancement Research Initiative (seari.mit.edu), a consortium of systems engineering leaders from industry, government, and academia; and the Program on Emerging Technologies (PoET), an interdisciplinary research effort of the National Science Foundation at MIT.

References

---

[1] Neumann, P. (2000). "Practical Architectures for Survivable Systems and Networks." Prepared by SRI International for the U.S. Army Research Laboratory.

[2] Abraham, S. and R. Efford (2004). "Final Report on the August 14th Blackout in the United States and Canada." U.S.-Canada Power System Outage Task Force.

[3] Knabb, R., J. Rhome and D. Brown (2005). "Tropical Cyclone Report: Hurricane Katrina." National Hurricane Center.

[4] Rumsfeld, D., D. Andrews, R. Davis, H. Estes, R. Fogleman, J. Garner, W. Graham, C. Horner, D. Jeremiah, T. Moorman, D. Necessary, G. Otis and M. Wallop (2001). "Report of the Commission to Assess United States National Security Space Management and Organization."

[5] Sheffi, Y. (2005). *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*. Cambridge, The MIT Press.

[6] Hollnagel, E., D. Woods and N. Leveson (2006). *Resilience Engineering: Concepts and Precepts*. Hampshire, UK, Ashgate.

[7] Axelband, E., R. Valerdi, T. Baehren, B. Boehm, W. Brown, E. Colbert, D. Dorenbos, S. Jackson, A. Madni, G. Nadler, R. Robertson, P. Robitaille, S. Settles and T. Tran (2007). "A Research Agenda for System of Systems Architecting." 17th INCOSE Symposium, San Diego, CA.

[8] Richards, M. (2009). "Multi-Attribute Tradespace Exploration for Survivability." Doctoral dissertation, Engineering Systems Division, Massachusetts Institute of Technology, Cambridge, MA.

[9] Fricke, E. and A. Schulz (2005). "Design for Changeability (DfC): Principles to Enable Changes in Systems Throughout Their Entire Lifecycle." *Systems Engineering*, 8(4): 342-359.

[10] McManus, H., M. Richards, A. Ross and D. Hastings (2007). "A Framework for Incorporating "ilities" in Tradespace Studies." *AIAA Space 2007*, Long Beach, CA.

[11] Richards, M. (2008). "'Complexity Has Bred Fragility': How Systems Engineering Can Enhance the Survivability of Space Systems." *INCOSE Insight*, 11(5): 19-21.

[12] Ball, R. (2003). *The Fundamentals of Aircraft Combat Survivability Analysis and Design*. Reston, American Institute of Aeronautics and Astronautics.

[13] Richards, M., D. Hastings, D. Rhodes and A. Weigel (2008). "Systems Architecting for Survivability: Limitations of Existing Methods for Aerospace Systems." *6th Conference on Systems Engineering Research*, Los Angeles, CA.

[14] Ross, A., D. Hastings, J. Warmkessel and N. Diller (2004). "Multi-Attribute Tradespace Exploration as Front End for Effective Space System Design." *Journal of Spacecraft and Rockets*, 41(1): 20-28.

[15] Ross, A. (2006). "Managing Unarticulated Value: Changeability in Multi-Attribute Tradespace Exploration." Doctoral dissertation, Engineering Systems Division, Massachusetts Institute of Technology, Cambridge, MA.

[16] CBO (2007). "Alternatives for Military Space Radar." Congressional Budget Office.

[17] USAF (2005). "SMC Systems Engineering Primer and Handbook." Space & Missile Systems Center, U.S. Air Force.

---

[18] Richards, M., A. Ross, D. Hastings and D. Rhodes (2008). "Two Empirical Tests of Design Principles for Survivable System Architecture." *18th INCOSE Symposium*, Utrecht, The Netherlands.

[19] Richards, M., A. Ross, D. Hastings and D. Rhodes (2008). "Empirical Validation of Design Principles for Survivable System Architecture." *2nd IEEE Systems Conference*, Montreal, Canada.

[20] Richards, M., A. Ross, D. Hastings and D. Rhodes (2009). "Survivability Design Principles for Enhanced Concept Generation and Evaluation." *19th INCOSE Symposium*, Suntec City, Singapore.

[21] Richards, M., A. Ross, N. Shah and D. Hastings (2008). "Metrics for Evaluating Survivability in Dynamic Multi-Attribute Tradespace Exploration." *AIAA Space 2008*, San Diego, CA.

[22] Richards, M., A. Ross, D. Hastings and D. Rhodes (2009). "Multi-Attribute Tradespace Exploration for Survivability." *7th Conference on Systems Engineering Research*, Loughborough, UK.

[23] Richards, M., A. Ross, D. Stein and D. Hastings (2009). "Multi-Attribute Tradespace Exploration for Survivability: Application to Satellite Radar." *AIAA Space 2009*, Pasadena, CA.