Multi-Attribute Tradespace Exploration for Survivability

Matthew G. Richards,[1] Adam M. Ross,[2] Daniel E. Hastings,[3] and Donna H. Rhodes[4]

[1] Massachusetts Institute of Technology, USA, mgr@alum.mit.edu
[2] Massachusetts Institute of Technology, USA, adamross@mit.edu
[3] Massachusetts Institute of Technology, USA, hastings@mit.edu
[4] Massachusetts Institute of Technology, USA, rhodes@mit.edu

Abstract
Multi-Attribute Tradespace Exploration (MATE) for Survivability is introduced as a system analysis methodology for improving the conceptual design of systems with critical survivability requirements. Multi-Attribute Tradespace Exploration for Survivability builds on the existing MATE process (i.e., a solution-generating and decision-making framework that applies decision theory to model-based design) by leveraging recent research on system survivability. In particular, seventeen survivability design principles (spanning susceptibility reduction, vulnerability reduction, and resilience enhancement strategies) and two value-based survivability metrics are incorporated into the concept generation and design alternative evaluation phases of MATE. At a high level, MATE for Survivability consists of eight steps: (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. To illustrate the methodology, examples are provided from a study of the survivability of alternative orbital transfer vehicles to debris. Applying the survivability design principles and metrics to the existing MATE methodology serves both to augment the creativity of system designers and to improve the evaluation of those alternatives by enabling integrated trades among system lifecycle cost, performance, and survivability.

Keywords – survivability, resilience, concept generation, value-based design, trade studies

1 Introduction

Survivability is the ability of a system to minimize the impact of a finite-duration disturbance on value delivery [1]. The operational environment of engineering systems is increasingly characterized by disturbances which may asymmetrically degrade performance, particularly for interdependent infrastructure systems. While disturbances may originate from a wide range of synthetic and natural hostile environments, a universal challenge confronting systems engineers is the specification, development, procurement, operation, and maintenance of systems with critical survivability requirements [2]. While survivability engineering has a rich historical legacy (*e.g.*, orders-of-magnitude improvements in combat aircraft survivability over the past half-century), existing analytic frameworks are not well-suited to incorporating survivability as an active trade in the design process, to reflecting the dynamics of operational environments, or to capturing path dependencies in the survivability assessment [3].

To address these limitations, Multi-Attribute Tradespace Exploration (MATE) for Survivability is introduced as a methodology for system analysts to incorporate survivability considerations into conceptual design. MATE for Survivability extends the existing MATE process that applies decision theory to model-based design [4]. In particular, a validated set of seventeen survivability design principles [5,6] are incorporated into the front-end of MATE to ensure consideration of a broad set of survivable alternatives. Additionally, the survivability metrics of time-weighted average utility loss and threshold availability [7] are incorporated into the back-end of MATE to ensure that systems are evaluated in terms of both their performance at beginning-of-life and their performance over representative distributions of disturbance environments.

The paper consists of four sections. Following this introduction, the second section describes the eight steps comprising MATE for Survivability. Sample applications of the methodology to an orbital transfer vehicle are also provided to illustrate critical steps. The third section provides a high-level review of the methodology and a discussion of the implications of MATE for Survivability to systems engineering. The fourth section concludes the paper with a brief summary.

2 Methodology Overview

The proposed methodology provides system analysts a structured approach for determining how a system can maintain value delivery across operational environments characterized by disturbances. The intent of the process is to couple the benefits of Multi-Attribute Tradespace Exploration in conceptual design with the benefits offered by the survivability design principles and the survivability metrics. In particular, MATE for Survivability is a value-driven process in which the designs under consideration are directly traced to the value proposition, and the measures-of-effectiveness reflect the preferences of the decision-

maker during nominal and perturbed environmental states. By following a parametric modeling approach, broad exploration of the tradespace is enabled in which the decision-maker gains an understanding of how their value proposition maps onto a large number of alternative system concepts. By emphasizing breadth rather than depth, promising areas of the tradespace may be selected with confidence for further analysis, and sensitivities between survivability design variables and disturbance outcomes may be explored. Figure 1 provides a flow chart of the process and identifies relationships with the legacy MATE process.

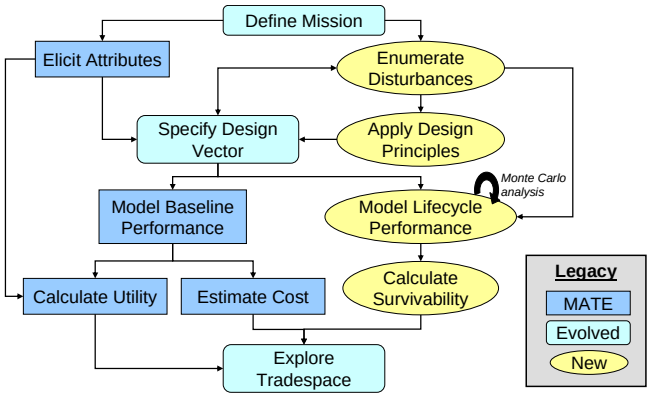

Figure 1 – *Multi-Attribute Tradespace Exploration for Survivability*

The eight phases are briefly described below, followed by a more detailed description in the subsequent subsections.

1. **Elicit value proposition** – Identify mission statement and quantify decision-maker needs during nominal and emergency states.
2. **Generate concepts** – Formulate system concepts that address decision-maker needs.
3. **Characterize disturbance environment** – Develop concept-neutral models of disturbances in operational environment of proposed systems.
4. **Apply survivability principles** – Incorporate susceptibility reduction, vulnerability reduction, and resilience enhancement strategies into design alternatives.
5. **Model baseline system performance** – Model and simulate cost and performance of design alternatives to gain an understanding of how decision-maker needs are met in a nominal operational environment.
6. **Model impact of disturbances on lifecycle performance** – Model and simulate performance of design alternatives across a representative sample of disturbance encounters to gain an understanding of how decision-maker needs are met in perturbed environments.
7. **Apply survivability metrics** – Compute time-weighted average utility loss and threshold availability for each design alternative as summary statistics for system performance across representative operational lives.
8. **Explore trades and refine analysis** – Perform integrated cost, performance, and survivability trades across design space to identify promising alternatives for more detailed analysis.

2.1 Elicit Value Proposition

The first phase of MATE for Survivability is focused on gaining a precise understanding of the value proposition for the system under analysis. This value proposition will drive the process of selecting and evaluating design alternatives. Five tasks comprise the first phase: (1.1) develop mission statement, (1.2) identify decision-maker, (1.3) elicit multi-attribute value function, (1.4) specify emergency value threshold(s), and (1.5) specify permitted recovery time(s).

Task 1.1 Develop Mission Statement

Developing a mission statement involves identifying the purpose for the creation of the system, stating the vision for the system development, and establishing boundaries for the system concepts to be considered. The goal of defining the mission is to clearly articulate stakeholder needs and the context in which a system is to be developed.

Task 1.2 Identify Decision-maker

As discussed in Ross *et al.* [4], MATE formalizes the inclusion of various stakeholders typically not considered by the design engineer. Depending on the purpose of the MATE study, these may include external policy stakeholders, organizational stakeholders, and system user stakeholders. In MATE for Survivability, the identification of a decision-maker is synonymous with identifying a representative customer stakeholder (which may be separate from end-user stakeholders) since this stakeholder controls the resources for the system development and is responsible for providing design requirements. If the system is dominated by multi-stakeholder considerations, it may be possible to identify a "benevolent dictator" decision-maker who seeks to create a successful system by balancing competing stakeholder requirements while remaining within budget.

Task 1.3 Elicit Multi-Attribute Value Function

Following Task 1.2, the system analyst engages with the decision-maker to extract objectives from the mission statement. Attributes are defined by the decision-maker as quantifiable parameters for measuring how well decision-maker-defined objectives are met.[1] In lieu of fixed requirements to drive the design process, acceptability ranges for each attribute are elicited (where the minimally acceptable level becomes a requirement and extra value is delivered for exceeding that level). In order to satisfy the axioms of Multi-Attribute Utility Theory [8], the analyst must ensure that the attribute set is defined by the decision-

[1] Attributes must be complete, operational, decomposable, non-redundant, minimal, and perceived independent [8].

maker; including precise definitions for each attribute with units, an acceptability range, and a monotonic preference for the direction of increasing goodness.

Having agreed to a set of attributes and acceptability ranges, the analyst next elicits the single-attribute utility functions to assess the amount of value provided to the decision-maker for a particular level of attribute. Utility is an ordinal metric (ranging from 0 to 1) that captures the preferences of the decision-maker across the acceptable attribute levels in the presence of uncertainty [9]. For systems that have multiple attributes, computing a single scalar value function that fully reflects decision-maker preferences can be difficult. As a proxy for value, the multi-attribute utility function, as defined in Keeney and Raiffa [8], is used to reflect preference orderings:

$$KU(\underline{X})+1=\prod_{i=1}^{N}[Kk_iU_i(X_i)+1] \quad for \quad K\neq 0$$

$$or \quad U(\underline{X})=\sum_{i=1}^{N}U(X_i) \quad for \quad K=0$$

where K is the solution to

$$K+1=\prod_{i=1}^{N}[Kk_i+1];$$

$$\sum_{i}^{N}k_i<1 \quad K>0$$

$$\sum_{i}^{N}k_i>1 \quad -1<K<0$$

$$\sum_{i}^{N}k_i<1 \quad K=0$$

The issue of stakeholder value elicitation is core to the MATE process and well-documented in existing literature. Ross [10] provides a detailed explanation of the multi-attribute utility function and a description of recommended techniques for eliciting the single-attribute and multi-attribute utility functions (*i.e.*, lottery equivalent probability method and corner point interviews, respectively). To examine the trade-off between rigor and ease of implementation, Spaulding [11] discusses the implications of simplifying the elicitation of single-attribute utility functions using hand-drawn utility curves and linear, risk-averse preference relationships.

Task 1.4 Specify Emergency Value Threshold

To incorporate survivability considerations into the need identification phase, it is necessary to elicit changing decision-maker expectations across disturbance environments. 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 [12].

One implication of value thresholds changing as a function of the environment is that the definition and scale of the utility axis will vary across nominal and perturbed environment states. A general response to this implication is to elicit applicable multi-attribute utility functions across all potential environments from the decision-maker. However, depending on the particular system under analysis and the decision-maker, it may be possible to assume that the attributes comprising the utility functions are constant (with variation only on in terms of acceptability ranges and scaling of the single-attribute utility functions). Therefore, the analyst should inquire whether the lower bounds of attribute acceptability may be temporarily broadened in the presence of finite-duration disturbances and, if so, the magnitudes associated with that extension.

As in the process of eliciting utility functions during nominal conditions, the process of eliciting attribute acceptability ranges during disturbance events requires the analyst to engage in a scenario-based dialogue with the decision-maker (*e.g.*, following the loss of satellite X before the launch of satellite Y, can you accept a higher maximum acceptable revisit time for ground targets?). This scenario-based dialogue may help to place the decision-maker in the proper mindset for the utility interview and help the analyst determine whether different emergency value thresholds need to be elicited for each disturbance type.

Task 1.5 Specify Permitted Recovery Time

Establishing the duration of the emergency value threshold defines the boundaries for system recovery. In performing this activity, it is useful to understand the time constants associated with performing the mission of the system under investigation (*e.g.*, availability requirements for on-demand operations). In the limit that the permitted recovery time goes to zero, the required value threshold is operable over the entire system life.

2.2 Generate Concepts

In the first phase, the MATE for Survivability methodology was initialized by eliciting the value proposition for the system under analysis. In the second phase of concept generation, analysts and engineers formulate the design effort by explicitly linking back to the value proposition. Four activities comprise the second phase: (2.1) identify constraints, (2.2) propose design variables, (2.3) map design variables to attributes, and (2.4) finalize baseline design vector.

Task 2.1 Identify Constraints

Constraints are requirements that must be satisfied in order to be feasible. Constraints may derive from physical laws, concepts-of-operations, policy (*e.g.*, requirement to use domestic launch vehicles), and environmental considerations (*e.g.*, minimum practical orbit altitude to

avoid atmospheric drag). As demonstrated in Ross [13], some constraints are subject to change and must be carefully tracked as shifts may significantly alter the "best" outcome for a particular problem.

Task 2.2 Propose Design Variables

The concept generation phase of tradespace exploration is concerned with the mapping of form to function. In thinking through solutions for how the attributes might be acquired, the designer inspects the attributes and proposes various design variables (and associated ranges and enumerations). Design variables are designer-controlled quantitative parameters that reflect an aspect of a concept, which taken together as a set uniquely define a system architecture. Each combination of design variables constitutes a unique design vector, and the set of all possible design vectors constitutes the design-space. In the process of proposing design variables, a natural tension exists between including more variables to analyze larger tradespaces and the computational limits on evaluating a larger set of designs.

Task 2.3 Map Design Variables to Attributes

Design variables are mapped to the attributes to ensure that the system concepts address the needs articulated by the decision-maker. As illustrated in Table 1, this mapping consists of a qualitative assessment in which a modified Quality Function Deployment process is followed. (The qualitative assessments may be revisited after models have been developed in Task 5.2.)

Table 1 - *Design Value Mapping Matrix*

Attributes	Design Vars: Propulsion System	Fuel Load	Equipment Mass	Total
Delta-V	9	9	9	27
Speed	9	1	1	11
Equipment Capability	0	0	9	9
Total	18	10	19	

Four general steps comprise mapping the design variables to attributes. First, a matrix is drawn with the elicited attributes as rows and the proposed design variables as columns. Second, estimates regarding the strength of the relationship between the design variables and attributes are made in the intersecting cells. Typically, a non-linear scale is used: 0 (no impact), 1 (low impact), 3 (medium impact), and 9 (strong impact). Third, the columns are summed to provide an estimate of the importance of a particular design variable. (An aggregate sum is computed for each design variable column as an indicator of the importance of its inclusion in the design-space. The size of the tradespace grows geometrically as design variables are added, requiring the pre-screening of design variables if limited computing resources are available.) Fourth, the rows are summed to provide an estimate of the degree to which each attribute is addressed by the proposed set of design variables. Verifying that each attribute is affected by the design variable under consideration is crucial to ensure that the trade study includes concepts that are traced to the value proposition of the decision-maker.

Task 2.4 Finalize Baseline Design Vector

The concept generation phase is completed with the finalization of the design variables, including the range and step size for each design variable (*e.g.*, Table 2). Whether discrete or continuous, the selection of the number of steps for a given design variable may be broken into the enumeration phase and the sampling phase. In the enumeration phase, a "full" range of values is selected that will drive the dependent variables across a large range. In the sampling phase, a subset of values in the enumerated range is selected for inclusion in the tradespace analysis. The sampling phase is necessary to efficiently utilize finite computing resources.

Table 2 - *Baseline Design Vector (n=128)*

Manipulator Mass	Propulsion Type	Fuel Load (kg)
Low (300kg)	Storable bi-prop	30
Medium (1000kg)	Cryogenic bi-prop	100
High (3000 kg)	Electric (NSTAR)	300
Extreme (5000 kg)	Nuclear Thermal	600
		1200
		3000
		10000
		30000

2.3 Characterize Disturbance Environment

Following completion of the first iteration of concept generation in a typical tradespace study, the analyst models and simulates the design alternatives to calculate the costs and utilities of alternative concepts. However, in MATE for Survivability, it is first necessary to characterize any disturbances in the operational environment (Phase 3) and to apply the survivability principles to the tradespace (Phase 4). Phase 3 is comprised of three tasks: (3.1) enumerate disturbances, (3.2) gather data on disturbance magnitude and occurrence, and (3.3) develop system-neutral models of disturbance environment.

Task 3.1 Enumerate Disturbances

The first step of applying the design principles is to enumerate potential disturbances. Prior to consulting the design principles, this step is necessary to provide context to the survivability analysis. Data for the system threat assessment may be derived from a combination of causal methods, historical data, scenario planning, and aggregated expert opinion (*e.g.*, Bayesian treatment, Delphi technique, interactive approach).

Task 3.2 Gather Data on Disturbance Frequency

Task 3.2 is to gather data on the magnitude and occurrence of different disturbance types to support subsequent model development (*e.g.*, Figure 2). Just as each attribute may vary in importance to the decision-maker, the impact of each type of disturbance on system performance may vary.

If all disturbances are not of equal concern, an importance score for each disturbance is assigned based on the magnitude of impact and likelihood of occurrence.

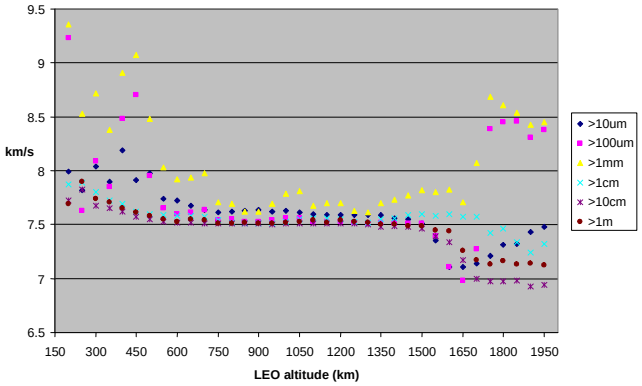

Figure 2 - *Average Orbital Velocity for LEO Debris*

In the process of gathering data on disturbance magnitude and occurrence, it is important to check for non-additive disturbance interactions (*e.g.*, in the case of a combat aircraft, the combination of an adversary jamming warning sensors and firing a missile will impact the system more than each disturbance in isolation). If multiple disturbances are likely to occur together and impact the system in a nonlinear way, such combinations of disturbances should be treated as separate disturbances. (In the case of intelligently-engineered disturbance environments, such interactions may be common.)

Task 3.3 Develop System-Neutral Disturbance Models

Having gathered data to characterize the disturbance environment, it is necessary to organize, structure, and format the data for subsequent disturbance modeling. Given the baseline system concept developed in Phase 2 and knowledge of the disturbance environment, descriptive models of each disturbance type are created. The models are parametric in nature to allow application to all design vector variations within a given system concept.

2.4 Apply Survivability Principles

After the baseline set of design variables is established and the disturbance environment is characterized, the survivability design principles are applied to the tradespace. Applying the design principles (Phase 4) supplements the concept generation activities in Phase 2 by incorporating survivability strategies that mitigate the disturbances identified in Phase 3. This phase consists of five steps: (4.1) enumerate survivable concepts from design principles, (4.2) parameterize survivable concepts with design variables, (4.3) assess ability of design variables to mitigate disturbances, (4.4) filter survivability design variables, and (4.5) finalize design vector.

Task 4.1 Enumerate Survivable Concepts from Principles

A set of seventeen survivability design principles (Table 3) are consulted to inform the generation of system concepts that mitigate the impact of each disturbance. Each design principle provides a concept-neutral architectural strategy for achieving survivability. These architectural strategies include both structural principles (*e.g.*, distribution, heterogeneity) as well as behavioral principles (*e.g.*, prevention, avoidance). To instantiate these design principles, the designer must select how each structural or behavioral principle may be represented in a concept (*i.e.*, the encapsulation of a mapping of function to form).

Figure 3 illustrates how susceptibility reduction,

Table 3 - *Seventeen 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

vulnerability reduction, and resilience enhancement strategies are incorporated into the design vector of the "space tug" orbital transfer vehicle.

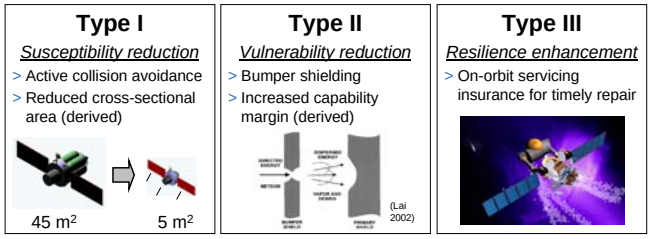

Figure 3 - *Survivability Concepts for Space Tug*

Task 4.2 Parameterize Survivable Concepts

To operationalize the proposed survivability concept enhancements for tradespace exploration, each concept is parameterized by specifying a representative set of design variables. While concepts are *qualitative* descriptions of system strategies, design variables are *quantitative* parameters that represent an aspect of a concept that can be controlled by a designer. Each design variable includes units and an enumerated range of values for analysis. Determining the enumeration range for each survivability feature is informed by data on disturbance magnitude and occurrence.

Given the competing desires for including more design parameters to explore larger tradespaces while minimizing the computational constraints associated with modeling an excessive number of design vectors, both a reasonable number of design variables and a reasonable number of steps (for continuous variables) must be chosen. To reduce the total number of design variables considered, the baseline set of design variables is consulted, utilizing existing design variables where possible in the process of concept parameterization.

Task 4.3 Assess Mitigating Ability of Design Variables

The ability of candidate survivability design variables to mitigate the impact of system disturbances is assessed to determine which design parameters to include in the system model. Estimating the degree of impact of each survivability design variable on each disturbance type follows a process analogous to the design value mapping matrix (where the ability of proposed design variables to impact the attributes is evaluated).

If multiple design variables and disturbances require assessment, a matrix of survivability design variables (rows) and disturbances (columns) may be structured with the strength of relationship assessed in intersecting cells (*e.g.*, 0, 1, 3, 9). In the process of building the matrix to estimate the effectiveness of the survivability design variables, it may be necessary to consolidate redundant design variables. While most survivability enhancement concepts are specified by a unique design variable or set of design variables, a few design variables may serve to parameterize more than one principle and concept. In consolidating duplicate design variable rows in the survivability design matrix, the maximum mitigating impact score for each disturbance is kept.

4.4 Filter Survivability Design Variables

After applying the design principles to incorporate survivability considerations into concept generation, it may be necessary to filter the expanded number of design variables for inclusion in the tradespace. This filtering process begins by examining the representation of the seventeen design principles across the consolidated set of design variables. While it may not be wise or possible to include design variables spanning all seventeen design principles (*e.g.*, tension of many susceptibility reduction and vulnerability reduction features), it is useful for the system analyst to understand the implications of including or excluding particular design variables on the tradespace. For example, design variables which utilize multiple principles should receive particular consideration for inclusion. Also, if the operational environment of the system being designed is highly uncertain, it may be wise to ensure representation of Type I, Type II, and Type III survivability trades in the design-space.

If multiple disturbances are included in the system analysis, it is necessary to aggregate the impact of each consolidated design variable across the disturbances. For example, a linear-weighted sum for each survivability design variable may be computed by summing across the rows in the survivability design matrix, weighting each disturbance based on the importance score in Task 3.2.

Task 4.5 Finalize Design Vector

Finalization of the design variables is required before initiating modeling and simulation of the design alternatives. Table 4 shows the finalized design vector for a space tug, incorporating three survivability design variables that increase the number of alternatives by a factor of twenty.

Table 4 - *Space Tug Design Options (n=2560)*

Manipulator Mass
Low (300kg)
Medium (1000kg)
High (3000 kg)
Extreme (5000 kg)

Propulsion Type
Storable bi-prop
Cryogenic bi-prop
Electric (NSTAR)
Nuclear Thermal

Fuel Load (kg)
30
100
300
600
1200
3000
10000
30000

Shield Mass (kg)
30
100
300
500
1000

Servicing
no
yes

Collision Avoidance
no
yes

survivability features

Finalizing the design vector requires an understanding of the relationship between the design variables and attributes as well as between the design variables and disturbances. Several considerations are recommended for determining which survivability design variables to incorporate into the

baseline design vector: the aggregate mitigating impact score of a particular design variable, the distribution of design variables across survivability design principles, downstream computational constraints of growing the design-space, and whether a particular survivability enhancement feature should be permanently turned "on" *(i.e.*, making survivability enhancement features that are certain to be incorporated into design constants).

2.5 Model Baseline System Performance

In Phase 5, the lifecycle cost and design utility (*i.e.*, utility at beginning-of-life) of each design alternative is computed by evaluating the design vector in a physics-based, parametric model. This phase consists of four steps: (5.1) develop software architecture, (5.2) translate design vectors to attributes, (5.3) translate design vectors to lifecycle cost, and (5.4) apply multi-attribute utility function.

Task 5.1 Develop Software Architecture

The initial mapping of design variables to attributes during concept generation (Task 2.3) consisted of using judgment and experience to determine which design variables to include in the trade study. In developing the software architecture, this mapping is performed at higher fidelity in which an N-squared matrix documents how design variables will be translated to attributes through intermediate variables (Table 5). Modules within the matrix enable the model to be decomposed and developed in parallel.

Table 5 - *N^2 Matrix for Space Tug Software Architecture*

	Constants	Generate Space Tugs	Propulsion Attributes	Grappling Attribute	Utility	Lifecycle Cost	Shielding Effectiveness	Impact Events	Outputs
Constants									
Generate Space Tugs	X								
Propulsion Attributes	X	X							
Grappling Attribute	X	X							
Utility			X	X					
Lifecycle Cost	X	X							
Shielding Effectiveness	X	X							
Impact Events	X	X					X		
Outputs	X	X	X	X	X	X	X	X	

Task 5.2 Translate Design Vectors to Attributes

Following completion of the software architecture, the sampling plan of the design variables is determined. (Due to the geometric growth of the tradespace, multi-disciplinary optimization techniques may be required in lieu of a full-factorial sampling.) This sampling of the tradespace is then input to the parametric computer model which calculates the set of attribute values for each design vector.

Task 5.3 Translate Design Vectors to Lifecycle Cost

In addition to translating design variables to attributes, the model also translates design variables to estimates of lifecycle cost. Developing cost models during the conceptual design phase of complex systems is a challenge. While detailed bottom-up estimating may be accurate for established programs, it is a weak method for systems with immature designs and low technology readiness. Analogy-based estimating may be applied only if similar systems exist. When known physical, technical, and performance parameters can be related to cost, the parametric costing method is best for conducting conceptual designs under time constraints [14].

Task 5.4 Apply Multi-Attribute Utility Function

Having calculated the performance of design alternatives across the attributes of concern to the decision-maker, these attribute levels are input to the elicited utility functions to arrive at an overall assessment of decision-maker satisfaction.

2.6 Model Impact of Disturbances on Performance

Phase 6 involves modeling and simulating the performance of design alternatives across a representative sample of disturbance encounters to gain an understanding of how decision-maker needs are met in perturbed environments. While the previous phase is focused on assessing deterministic measures of system effectiveness (*i.e.*, lifecycle cost, design utility), this phase focuses on determining the distributions of the survivability metrics (*i.e.*, time-weighted average utility, threshold availability) from a probabilistic simulation. Phase 6 consists of four tasks: (6.1) calculate stochastic susceptibility, (6.2) model probabilistic vulnerability, (6.3) model probabilistic recovery, and (6.4) generate distributions of utility trajectories.

Task 6.1 Calculate Stochastic Susceptibility

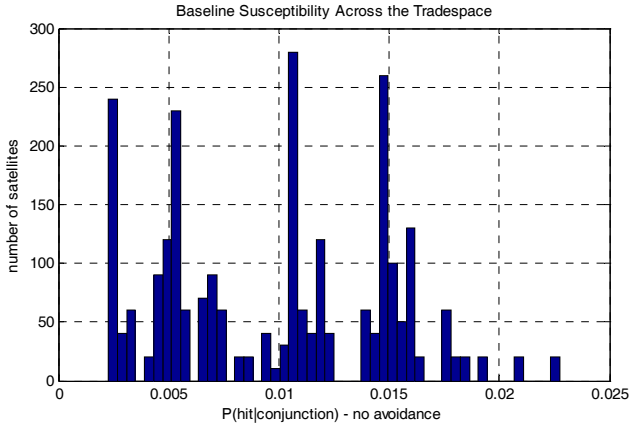

Figure 4 - *Distribution of Outcomes from Debris Conjunction Events*

Having gathered data and developed a system-independent model of the disturbance environment (*e.g.*, debris flux as a function of mass per m^2) in Task 3.3, a system-dependent model of the disturbance environment is created (*e.g.*,

debris flux as a function of mass per exposed cross-sectional area). If disturbances occur probabilistically, a Monte Carlo analysis is conducted to generate representative distributions of disturbance timelines for the design vectors. Before accounting for survivability design variables, Figure 4 shows the baseline susceptibility of the 2560 in the space tug tradespace.

Task 6.2 Model Probabilistic Vulnerability

Given that a disturbance has affected the system, the impact of the disturbance is characterized through a probabilistic vulnerability model. Since there may only be mid-fidelity characterizations of the environment and system during conceptual design, the damage assumptions are often coarse (*e.g.*, Table 6).

Table 6 - *Debris Impact Outcomes*

debris diameter	1 mm ⟵x cm⟶ 10 cm			
	micro	small	medium	large
impact outcome	degradation	damage	severe damage	satellite loss
modeling assumption (7 km/s)	no impact	10% chance of loss in capability level	loss in capability level	end-of-life / collision avoidance with 99% success

The vulnerability model is a probabilistic lottery in which multiple runs are required to extract the distribution of potential outcomes. Although static, the vulnerability model is only called when directed by the stochastic susceptibility model to capture the dynamics of utility loss over the lifecycle. Path-dependencies are incorporated into the vulnerability model by transitioning between pre-enumerated degraded states in the case of non-catastrophic losses.

Task 6.3 Model Probabilistic Recovery

Given the occurrence of a disturbance, system degradation in the vulnerability model, and incorporation of Type III survivability design principles in the design vector, system recovery is modeled. As with the vulnerability model, the recovery model is a lottery in which outcomes are determined probabilistically and require multiple runs to determine central tendency. In the case of partial recovery, path-dependencies are incorporated by transitioning among pre-enumerated states.

For space tug design vectors incorporating a servicing option, an on-orbit repair mission is attempted following non-catastrophic debris hits. Successful servicing missions fully restore grappling capability to the original (baseline) level in the design vector.

Task 6.4 Generate Distributions of Utility Trajectories

As defined in the introduction, survivability is the ability of a system to maintain value delivery within stakeholder-defined thresholds over the lifecycle of a disturbance. Tradespace exploration for survivability operationalizes this definition by evaluating utility performance of alternative designs across disturbance events. These utility trajectories are plotted over time with any applicable value thresholds and permitted recovery times to characterize survivability. Because utility trajectories are probabilistic and path-dependent in nature, a Monte Carlo analysis is performed to generate representative distributions.

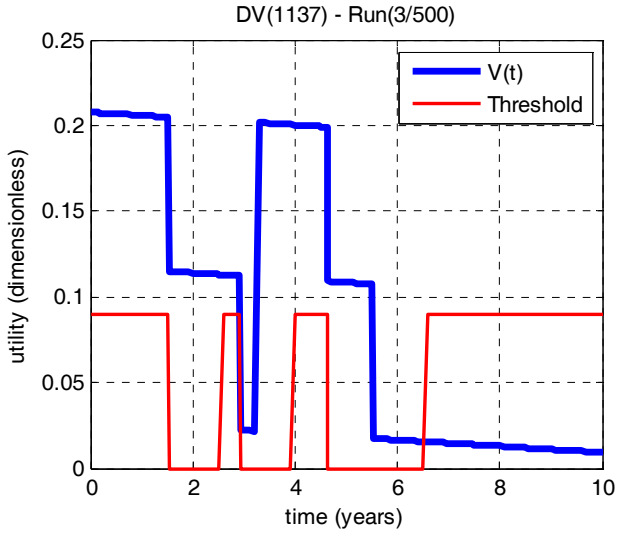

Figure 5 - *Sample Utility Trajectory Output from Dynamic State Model*

Survivability is an emergent system property which may be defined as the ability of a system to maintain value delivery within stakeholder-defined thresholds over the lifecycle of a disturbance. A dynamic space tug model operationalizes this definition by simulating utility trajectories of alternative designs in the presence of orbital debris events. Figure 5 presents a sample utility trajectory output from the model, illustrating *V(t)* (*i.e.*, dynamic multi-attribute utility) over a possible 10-year operational life. Following normal degradation during the first eighteen months of operation, two non-catastrophic debris impacts occur in succession. Due to the reduction in expectations from the required value threshold to the emergency value threshold following the first impact (and renewed following the second impact), *V(t)* does not pass below the value threshold. The first debris impact prompts a request for servicing that is successfully filled during the second year. A similar sequence of disturbances—consecutive debris hits followed by successful servicing—occurs between the fourth and sixth years. In this case, however, no servicing occurs and the system fails to meet the required value threshold when expectations are reset to the required value threshold.

As survivability is a stochastic, path-dependent property, the outcome of any particular run for a given design vector 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. Furthermore, there is a need to distinguish across collections of utility trajectories of different design vectors. However, observing all 128,000

utility trajectories—500 runs of each of the 2560 design vectors—is not practical from a decision-making perspective. Therefore, the survivability metrics are applied as aggregate measures for each set of utility trajectories.

2.7 Apply Survivability Metrics

Having generated utility trajectories over the distribution of possible degradation and recovery sequences for each design vector, summary statistics are collected to measure central tendency of lifecycle survivability. Phase 7 consists of three tasks: (7.1) establish percentile reporting levels, (7.2) calculate time-weighted average utility, and (7.3) calculate threshold availability. Before describing the three tasks of Phase 7, the survivability metrics of time-weighted average utility loss and threshold availability are briefly described. Previous work [7] provides a detailed motivation and derivation.

Survivability metrics with construct validity for the survivability definition [1] requires evaluating a system's ability both to minimize utility losses and to meet critical value thresholds before, during, and after disturbances. Given a characterization of a system's value delivery over time, $V(t)$, using a multi-attribute utility function, $U(t)$, the time-weighted average utility loss may be defined:

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

Time-weighted average utility loss may be used to assess the difference between the beginning-of-life, design utility, U_o, and the time-weighted average utility achieved by a system across operational environments during its design life, T_{dl}. However, while this metric enables continuous evaluations to be made across systems regarding ability to minimize degradation, it does not internalize the ability to meet critical value thresholds.

Threshold availability, A_T, evaluates the ability of a system to meet critical value thresholds. A_T is defined as the ratio of mean time above thresholds *MTAT* to the total design life:

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

Task 7.1 Establish Percentile Reporting Levels

The output of the survivability simulation is a distribution of utility trajectories for each design alternative. To enable comparisons among design alternatives, it is necessary to extract measures of central tendency from the utility trajectories. Time-weighted average utility loss and threshold availability are intended to provide these measures. However, experience indicates that the distributions of the survivability metrics are often highly-skewed, suggesting the use of percentiles rather than potentially misleading measures of central tendency such as average. To determine what percentile level to use (*e.g.*, time-weighted average utility–5th percentile is the level of time-weighted average utility achieved by 95% of the simulation runs of that design vector), the analyst must incorporate two considerations. First, the selected percentiles will ideally show variation across the tradespace to allow the decision-maker to discriminate among design alternatives using the survivability metrics. Second, the selected percentiles will reflect decision-maker risk preferences (where risk aversion manifests in the selection of lower percentiles). Selection of the percentile reporting levels is an iterative process with Task 8.1, exploring the multi-dimensional tradespace.

Task 7.2 Calculate Survivability Metrics

The percentile reporting levels are applied to the distributions of the two survivability metrics, adding two probabilistic quantities for inclusion with the deterministic metrics of lifecycle cost and design utility in the tradespace.

2.8 Explore Tradespace

The final phase focuses on tradespace exploration: (8.1) conduct integrated cost, utility, and survivability trades and (8.2) select design for further analysis.

Task 8.1 Conduct Integrated Tradespace Exploration

The purpose of tradespace exploration is to map the decision-maker preferences in the value domain onto the space of possible designs in the value domain. Traditionally, these are presented in a cost-benefit format in which multi-attribute utility is plotted against lifecycle cost (in accordance with the philosophy of cost as an independent variable). With technically diverse designs evaluated against a common set of attributes, unified trades may be made and interesting designs (*e.g.*, Pareto-optimal) may be flagged for more detailed analysis.

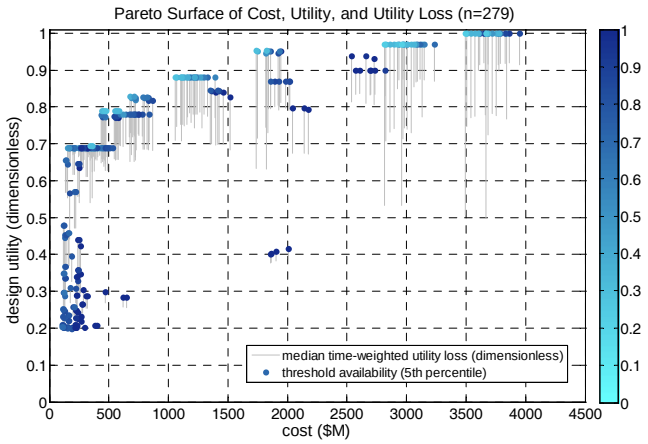

Figure 6 - *Three-Dimensional Pareto Surface of Survivability Tear Tradespace*

In conducting tradespace exploration for survivability, the probabilistic survivability metrics of time-weighted average utility loss and threshold availability are integrated with the cost-utility metrics using a survivability tear(drop) tradespace representation (*e.g.*, Figure 6). Decision-makers

may choose to navigate the tradespace by examining designs near the top-left (high utility, low cost) with high availability (darker) and minimal utility loss (shorter tail). As illustrated in Figure 6, nearly 90% of the tradespace is filtered (from 2560 to 279) by only plotting the points on the Pareto-efficient surface that meet the objectives of minimizing cost, maximizing design utility, and minimizing utility loss.

Task 8.2 Select Designs for Further Analysis

In the final task, the broad knowledge gained from exploring the tradespace may be applied to a variety of activities: magnification of a particular region of the tradespace by reducing the range and decreasing the step size of design variables, sensitivity analysis of uncertain model parameters, and the selection of a medium number of design vectors for higher-fidelity modeling.

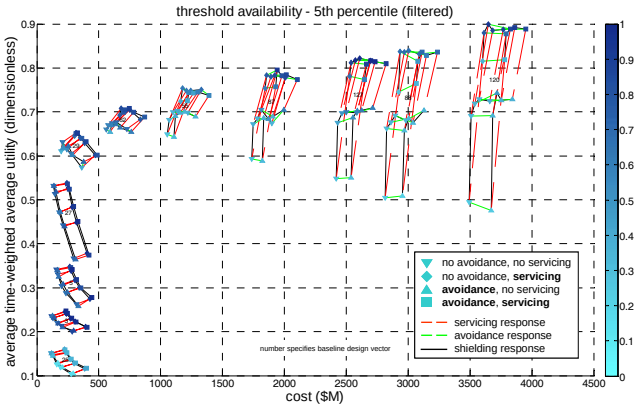

Figure 7 - *Survivability Response Surfaces along Pareto-Front of Cost and Average Utility*

For example, Figure 7 shows how a survivability response surface analysis may be conducted to assess how the various survivability design variables affect performance across the survivability metrics. This analysis may be conducted on specific designs for prescriptive insights as well as across the entire tradespace to reveal general trends.

3 Discussion

As described in the previous section, MATE for Survivability is an eight-phase process comprised of 29 tasks. Table 7 presents a Task Structure Matrix representation of MATE for Survivability to provide a bird-eye view of the entire process and to indicate dependencies among tasks. (To distinguish MATE for Survivability from the baseline MATE process, task numbers that are unique to the survivability extension are in bold font.) Each row consists of a particular task with "X" marks specifying inputs to that task. Above diagonal marks indicate feedback from subsequent tasks. For example, insights from conducting cost-utility-survivability trades in Task 8.1 may inspire numerous changes to the formulation of the design problem.

The Task Structure Matrix representation illustrates the highly-coupled nature of conceptual design activities. Given the extensive feedback of tradespace exploration (Phase 8) to previous tasks, Table 7 underscores the importance of pursuing modeling and simulation activities at a level of fidelity that is consistent with being able to conduct several iterations of the overall process.

Both the survivability design principles [5,6] and metrics [7] are fully integrated into MATE for Survivability. The process for incorporating survivability considerations within the design formulation phases (3 and 4) constitutes a top-down approach for consulting the design variables and generating concepts that may be better equipped to operate in the presence of environmental disturbances. The benefits

Table 7 - *Task Dependencies of MATE for Survivability*

Task	1.1	1.2	1.3	**1.4**	**1.5**	2.1	2.2	2.3	2.4	**3.1**	**3.2**	**3.3**	**4.1**	**4.2**	**4.3**	**4.4**	4.5	5.1	5.2	5.3	5.4	**6.1**	**6.2**	**6.3**	**6.4**	**7.1**	**7.2**	**8.1**	8.2
Develop mission statement	1.1		X																										
Identifiy decision maker	1.2	X																											
Elicit multi-attribute value function	1.3	X	X																										
Specify emergency value threshold	**1.4**	X	X	X																									
Specify permitted recovery time	**1.5**	X	X	X	X																								
Identify constraints	2.1	X	X					X																				X	
Propose design variables	2.2	X		X			X																					X	
Map design variables to attributes	2.3			X				X											X										
Finalize baseline design vector	2.4			X				X	X									X	X										
Enumerate disturbances	**3.1**	X								X																			
Gather data on disturbance magnitude and frequency	**3.2**										X																		
Develop model(s) of disturbance environment	**3.3**									X		X																	
Enumerate survivable concepts from principles	**4.1**									X	X																	X	
Parameterize survivable concepts with design variables	**4.2**									X		X		X															
Assess ability of design variables to mitigate disturbances	**4.3**										X	X			X														
Filter survivability design variables	**4.4**											X				X													
Finalize candidate design vectors	4.5									X							X		X	X		X						X	
Develop software architecture	5.1			X				X	X	X			X			X		X		X			X		X	X				
Translate design vectors to attributes	5.2			X			X		X									X	X										
Translate design vectors to lifecycle cost	5.3						X											X	X						X				
Apply multi-attribute value function	5.4			X																X									
Calculate stochastic susceptibility	**6.1**											X			X			X	X										
Model probabilistic vulnerability	**6.2**											X			X			X	X				X						
Model probabilistic recovery	**6.3**														X			X	X					X					
Generate distributions of utility trajectories	**6.4**				X	X																X		X	X				
Establish percentile reporting levels	**7.1**																									X			X	
Calculate average utility and theshold availability	**7.2**																									X	X		
Conduct integrated cost, utility, and survivability trades	**8.1**																			X	X							X	
Select designs for further analysis	8.2																												X

of the approach are twofold: (1) augment the creativity of system designers by ensuring consideration of a broad tradespace of design alternatives and (2) quickly screen and prioritize a large number of candidate design variables before proceeding to the design evaluation phase.

Application of the survivability metrics to the design evaluation phases (6, 7, and 8) allows integrated trades to be made by the decision-maker. In particular, the survivability metrics allow the decision-maker to discriminate among the large number of alternative designs in terms of sustained system performance across representative distributions of disturbance environments. These metrics operationalize the value-centric definition of survivability through three desirable characteristics: (1) value-based, to allow comparisons across technically-diverse system concepts, (2) dynamic, to allow assessment (and enhancement) of survivability across the lifecycle of a disturbance, and (3) continuous (rather than a discrete, binary characterization), to enable distinction between systems that gracefully degrade and those that fail immediately following a disturbance.

4 Conclusion

This paper introduced Multi-Attribute Tradespace Exploration for Survivability as a structured approach for evaluating design alternatives that will be operating in dynamic disturbance environments. In particular, recent research on survivability design principles and survivability metrics are incorporated into the existing MATE conceptual design methodology that applies decision theory to model-based design.

By incorporating survivability considerations into the conceptual design phase, MATE for Survivability stands in contrast to most survivability analysis methodologies which examine the cost-effectiveness of survivability features during detailed design. By incorporating survivability considerations before a baseline system concept has been established, MATE for Survivability allows survivability to be incorporated earlier and more effectively into product development.

5 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.

6 References

[1] Richards, M., D. Hastings, D. Rhodes and A. Weigel (2007), "Defining Survivability for Engineering Systems." *5th Conference on Systems Engineering Research*, Hoboken, NJ.

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

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] Keeney, R. and H. Raiffa (1993), *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*, Cambridge: Cambridge University Press.

[9] von Neumann, J. and O. Morgenstern (1953), *Theory of Games and Economic Behavior*, Princeton: Princeton University Press.

[10] Ross, A. (2003), "Multi-Attribute Tradespace Exploration with Concurrent Design as a Value-Centric Framework for Space System Architecture and Design," Dual Master's thesis, Department of Aeronautics and Astronautics, Technology and Policy Program, Massachusetts Institute of Technology, Cambridge, MA.

[11] Spaulding, T. (2003), "Tools for Evolutionary Acquisition: A Study of Multi-Attribute Tradespace Exploration (MATE) Applied to the Space Based Radar (SBR)," Master's thesis, Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, MA.

[12] Bayer, T. (2007), "Planning for the Un-plannable: Redundancy, Fault Protection, Contingency Planning and Anomaly Response for the Mars Reconnaissance Orbiter Mission," *AIAA Space 2007*, Long Beach, CA.

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

[14] Wertz, J. and W. Larson (1999), *Space Mission Analysis and Design*, El Segundo: Microcosm Press.

