Survivability Design Principles for Enhanced Concept Generation and Evaluation

Matthew G. Richards
Massachusetts Institute of Technology
77 Massachusetts Ave., Bld. 41-205
Cambridge, MA 02139
mgr@mit.edu

Adam M. Ross
Massachusetts Institute of Technology
77 Massachusetts Ave., Bld. E38
Cambridge, MA 02139
adamross@mit.edu

Daniel E. Hastings
Massachusetts Institute of Technology
77 Massachusetts Ave., Bld. 7-133
Cambridge, MA 02139
hastings@mit.edu

Donna H. Rhodes
Massachusetts Institute of Technology
77 Massachusetts Ave., Bld. E38
Cambridge, MA 02139
rhodes@mit.edu

Abstract. Survivability is the ability of systems to minimize the impact of finite-duration disturbances on value delivery. Previous work developed and tested a set of seventeen survivability design principles spanning susceptibility reduction, vulnerability reduction, and resilience enhancement strategies. In this paper, a process is described for applying the survivability design principles to the concept generation phase of Multi-Attribute Tradespace Exploration, a system analysis methodology integrating decision theory with model-based design. Applying the design principles serves both to augment the creativity of system designers by ensuring consideration of a broad tradespace of design alternatives and to quickly screen a large number of candidate design variables before proceeding to concept evaluation.

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 (Neumann 2000). Engineering systems are also vulnerable to unintelligent threats arising from the natural environment (Abraham and Efford 2004; Knabb, Rhome and Brown 2005). In response to these synthetic and natural disturbances, numerous studies and several government and academic research initiatives have been launched (Rumsfeld et al. 2001; Abraham and Efford 2004; Knabb, Rhome and Brown 2005; Sheffi 2005; Hollnagel, Woods and Leveson 2006; Axelband et al. 2007). 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. Within the aerospace and defense industries, survivability engineering application areas span strategic defense (Bennett 1980;

Canavan 1997), networked information systems (Baran 1964; Al-Noman 1998; Northrop et al. 2006), combat aircraft (Throndson 1982; Paterson 1999; Ball 2003), human spaceflight (Heydorn and Railsback 1999; Williamsen et al. 1999), missile defense (Canavan and Teller 1990; Lin 2003), satellite protection (Canavan 1989; Howard 1993; Nordin and Kong 1999), unmanned aerial vehicles (Ahn, Lee and Kim 2002; Jeffcoat 2003), and homeland security (Ball and Atkinson 2006; Perrow 2007). Numerous application areas exist outside of the aerospace and defense industries as well—ranging from immunization of individual organisms in the life sciences (Ellison et al. 1999) to the design of crashworthy Formula-One racing vehicles (Catchpole et al. 2007).

To incorporate survivability considerations into conceptual design, this paper introduces an approach for deploying an existing set of seventeen survivability design principles during concept generation (Richards et al. 2008a). As discussed in previous work, the intent of the design principles is to enhance concept generation by expanding the set of system design trade-offs under consideration. Several conceptual frameworks exist of survivability design strategies (Ellison, Fisher et al. 1999; Nakano and Suda 2007). However, most offer no guidance on operationalizing each strategy for concept generation and evaluation in engineering design. This offers a significant area to contribute to the literature given the criticality of front-end systems engineering activities (during which management leverage is highest and the majority of development resources tend to be committed) (Blanchard and Fabrycky 2006).

Following this introduction, the seventeen survivability design principles are reviewed, and an existing conceptual design methodology, Multi-Attribute Tradespace Exploration (MATE) (Ross et al. 2004), is briefly described. Next, an approach is outlined for integrating the survivability design principles with MATE. The approach is illustrated through an application of the principles to the concept generation of a satellite radar system operating in a harsh natural environment. The paper concludes with a discussion of implications of the methodology, implementation issues, and propositions for future work.

Key Concepts

Survivability Design Principles

According to Department of Defense (DoD) Regulation 5000.2-R, survivability consists of susceptibility, vulnerability, and recoverability (DoD 2002):

> ***Susceptibility***. The degree to which a weapon system is open to effective attack due to one or more inherent weakness (AP3.2.7).
>
> ***Vulnerability***. The characteristic of a system that causes it to suffer a definite degradation as a result of having been subjected to a certain level of effects in an unnatural hostile environment (AP3.2.5).
>
> ***Recoverability***. Following combat damage, the ability to take emergency action to prevent loss of the system, to reduce personnel casualties, or to regain weapon system combat mission capabilities (AP3.2.8).

Traditionally specified as a requirement in military systems, survivability is an increasingly

important attribute of all systems which must be robust to environments characterized by system-threatening disturbances. While disturbances may originate from a wide range of artificial and natural environments, a universal challenge confronting system architects is the specification, evaluation, and verification of systems with critical survivability requirements.

Previous work developed a set of seven design principles (*i.e.*, concept-neutral strategies of architectural choice) for reducing system susceptibility, reducing system vulnerability, and enhancing system resilience. Initially, twelve design principles were deduced based upon a case study of U.S. strategic defense during the Cold War and a generic system-disturbance representation (Richards et al. 2007). Subsequent research tested the validity of these results by inductively mapping the survivability features of existing systems (*e.g.*, A-10 Thunderbolt II combat aircraft, UH-60A Blackhawk helicopter) to the design principle set (Richards et al. 2008b). Results from these iterative mappings identified missing design principles and taxonomic imprecision in design principle definitions—informing an expanded set of seventeen design principles. The design principle set stabilized in subsequent empirical tests (*e.g.*, Iridium satellite system, F-16 combat aircraft) (Richards, Ross et al. 2008a). Table 1 categorizes and defines the seventeen design principles.

Table 1. 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

The enumeration of design principles is only a first step towards a general analysis methodology for the generation and evaluation of system survivability. While the design principles are helpful for aiding the creative brainstorming of a larger set of survivability techniques, they are not intended as a check for completeness. Rather, the enumeration provides designers with a

portfolio of options from which to consider a larger tradespace of survivable designs. The success of this portfolio of survivable design principles will vary with context. Designs that achieve a successful balance of survivability, performance, and cost will almost certainty incorporate a subset of the seventeen principles with varying emphasis.

Multi-Attribute Tradespace Exploration

One approach for evaluating the ability of design alternatives to achieve a balance between performance and cost is Multi-Attribute Tradespace Exploration, a conceptual design methodology that applies decision theory to model-based design (Ross, Hastings et al. 2004). Decoupling the design from the need through tradespace exploration, MATE is both a solution-generating as well as a decision-making framework. (The solution-generating aspect distinguishes MATE from traditional decision analyses techniques which focus only on the evaluation step.) Descended from the Generalized Information Network Analysis (GINA) methodology which applies metrics from information theory to the quantitative evaluation of communications spacecraft (Shaw, Miller and Hastings 2001), MATE draws on multi-attribute utility theory to expand the analysis to systems that cannot be modeled as information networks. Figure 1 provides an overview of the MATE process.

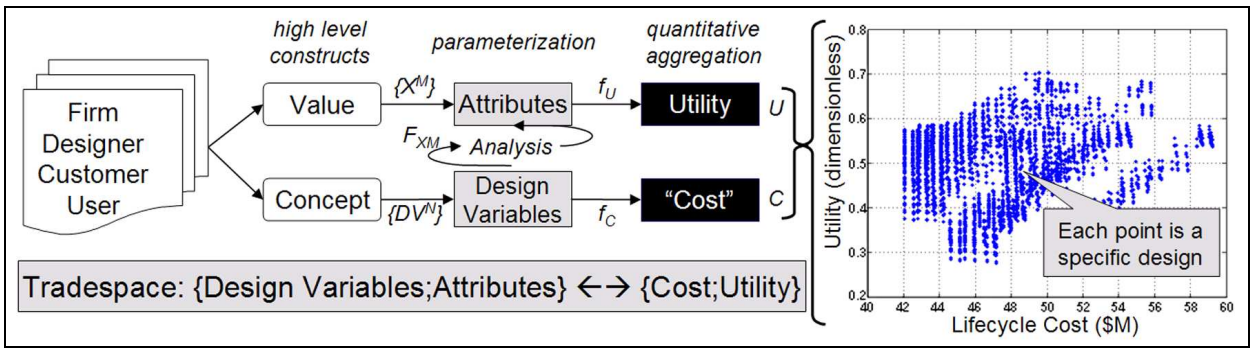

Figure 1. Multi-Attribute Tradespace Exploration (MATE) (Ross, Hastings et al. 2004)

MATE offers a promising baseline methodology for application of the survivability design principles given its ability to accommodate a diverse array of design alternatives. Rather than evaluating a few design alternatives at a high-level of fidelity, a typical MATE study utilizes computer-based parametric models and simulations to compare hundreds or thousands of potential architectures—providing the system analyst with a broad understanding of the design space. The sacrifice of depth for breadth is appropriate for the front-end evaluation of survivability enhancement features given the large number of design alternatives that may be generated from the portfolio of survivability design principles.

Integrating Survivability Design Principles with MATE

Ross (2003) provide a detailed description of the 48 steps in a MATE study. At a high level, the process consists of three general phases: need identification, concept generation, and design alternative evaluation. While all three phases of MATE are discussed below, this section focuses on how the survivability design principles may be leveraged to improve the concept generation phase. Emphasis is also given to the additional steps required of MATE to incorporate survivability considerations into the analysis. To illustrate the approach, a running example of a

satellite radar system operating in a harsh natural space environment is provided.

Initialize MATE

In the first phase of MATE, the mission needs and preferences of a decision maker[1] are defined and specified with attributes (*i.e.*, decision maker-perceived metrics that measure how well decision maker-defined objectives are met). Attributes, their associated acceptability ranges, and the amount of value provided to the decision maker for a particular level of attribute are elicited through formal utility interviews. Single-attribute utility curves are typically aggregated using aggregate, multiplicative utility function (a dimensionless metric of user satisfaction ranging from 0, minimally acceptable, to 1, highest of expectations).[2]

To incorporate survivability considerations into the need identification phase, it is also 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 (Bayer 2007). Therefore, the analyst should inquire whether the lower bounds of attribute acceptability may be broadened in the presence of finite-duration disturbances, and if so, the magnitude and time associated with that extension.

In the second phase of MATE, the attributes are inspected and various design variables and associated ranges and enumerations are proposed. (A design variable is a designer-controlled quantitative parameters that reflect aspects of a concept, which taken together as a set uniquely define a system architecture.) Each possible combination of design variables constitutes a unique design vector, and the set of all possible design vectors constitutes the design-space. This solution-generating phase—inspecting the decision maker-derived attributes to determine which design variables to include in the trade study—ensures that design activities in the technical domain are explicitly linked to the stakeholder needs elicitation in the value domain. Table 2 presents an example design value mapping matrix for a satellite radar system.

[1] As discussed in Ross (2004), 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. When only one stakeholder group is considered, the focus is typically on customer stakeholders (which may be separate from end-user stakeholders) since they control the resources for the system development and are responsible for providing design requirements.

[2] 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 (1993), can be used to reflect preference orderings.

Table 2. Design Value Mapping Matrix

			ATTRIBUTES															
			Mission										Programmatics					
			Tracking						Imaging					Cost		Schedule		
	Variable Name	Definition Range	Minimum Target RCS	Min. Discernable Velocity	Number of Target Boxes	Target ID Time	Target Track Life	Tracking Latency	Resolution (Proxy)	Targets per Pass	Field of Regard	Revisit Frequency	Imaging Latency	Baseline Cost	Actual Costs (Era)	Baseline Schedule	Actual Schedule (Era)	Total Impact
DESIGN VARIABLES	Peak Transmit Power	1.5 10 20 [KW]	9	9	9	3	1	1	9	9	9	0	1	9	9	9	9	**96**
	Radar Bandwidth	.5 1 2 [GHz]	9	9	3	3	1	1	9	9	9	0	1	3	3	3	3	**66**
	Physical Antenna Area	10 40 100 [m^2]	9	9	9	3	1	1	9	9	9	1	1	9	9	9	9	**97**
	Satellite Altitude	800 1200 1500 [km]	9	9	3	9	9	3	9	9	9	9	3	1	1	1	1	**85**
	Constellation Type	8 Walker IDs	0	0	1	9	9	3	0	0	3	9	3	9	9	9	9	**73**
	Comm. Downlink	Relay vs. Downlink	0	0	0	0	0	9	0	0	0	0	9	9	9	3	9	**48**
	Tactical Downlink	Yes vs. No	0	0	0	0	3	9	0	0	0	0	9	9	9	3	9	**51**
	Maneuver Package	1x, 2x, 4x	1	1	1	1	1	0	1	1	1	1	0	9	3	3	3	**27**
	Constellation Option	none, long-lead, spare	0	0	0	0	0	0	0	0	0	0	0	9	9	9	9	**36**
	Total		37	37	26	28	25	27	37	37	40	20	27	67	61	49	61	

In Table 2, the columns consist of attributes elicited from the decision maker and the rows consist of potential design variables for incorporation into the trade study. The intersecting cells—indicating the interaction between a design parameter and a stakeholder attribute—are scored on a "no impact," "low impact," "medium impact," and "high impact" scale (*i.e.*, 0, 1, 3, and 9, respectively). An aggregate sum is computed for each design variable row 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). In addition to informing selection of design variables for subsequent modeling and simulation (rows), the design value mapping matrix may also be used to check whether the selected design variables adequately drive value delivery across all of the stakeholder-derived attributes (columns).

Apply Survivability Design Principles

In a typical MATE study, the first iteration of the concept generation phase is complete following selection of a baseline set of design variables using the design value mapping matrix. However, in a MATE analysis for survivability, the survivability design principles may be applied to the concept generation phase before proceeding to design alternative evaluation. Applying the design principles involves ten steps: (1) enumerate potential disturbances and their relative importance, (2) check for non-additive disturbance interactions, (3) generate survivable concepts from design principles, (4) parameterize survivable concepts with design variables, (5) assess degree of impact of survivability design variables on each disturbance type, (6) consolidate redundant design variables, (7) examine coverage of consolidated design variables across design principles, (8) aggregate mitigating impact of each consolidated design variable across disturbances, (9) order design variables based on impact, and (10) down-select survivability design variables for inclusion in expanded design-space.

The first step of applying the design principles is to enumerate potential disturbances. Occurring before the design principles are consulted, the first 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). 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. Table 3 shows the environmental disturbances for a satellite operating in low-Earth orbit, based on Pisacane (2008). For example, aerodynamic drag forces from atomic oxygen in the upper atmosphere may degrade orbits and chemically erode surfaces (Tribble 2003). However, given that the circular orbits in the design vector begin at 800 km, this disturbance is of low importance to the design vector. In contrast, micrometeorites and debris are of serious concern for Earth-observing constellations.

Table 3. Environmental Disturbances

Disturbance	**Importance (1-10)**
Atmospheric drag fluctuations	1
Arc discharging	3
High-flux radiation	4
Micrometeorites/debris	7
Signal attenuation	5
Change in target definition	4
Failure of relay backbone	6
Loss of tactical ground node	2

Having enumerated disturbances types, the second step is 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. However, given the focus of the analysis here on rare, naturally occurring disturbances in the space environment, such interactions do not dominate the survivability analysis.

In the third step, the design principles 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). Given the baseline set of design variables and environmental disturbances, a variety of concept enhancements were brainstormed for the satellite radar mission. The first two columns of Table 4 illustrate this mapping. For example, the design principle of margin was applied to the satellite constellation as well as to four different spacecraft subsystems (*i.e.*, power generation, communications, propulsion, and data storage). The design principle of redundancy was also applied to different elements of the system architecture, including the satellite-level, constellation level, and ground segment. In all, 24

concepts were generated from 13 of the survivability design principles. (Given the focus on natural disturbances, the Type I survivability design principles that modify the observations, decision making, and actions of hostile actors were not applicable).

Table 4. Survivability Design Variable Mapping Matrix

					disturbances							
	design principles	concept enhancements	design variables (units)	enumerated range	atmospheric drag fluctuations	arc discharging	high-flux radiation	micrometeorites / debris	signal attenuation	change in target characteristics	loss of relay backbone	loss of ground node
Type I	prevention	reduce exposed s/c area	antenna area (m^2)	[10, 40, 100]	9	0	3	9	0	0	0	0
	mobility											
	concealment											
	deterrence											
	preemption											
	avoidance	s/c maneuvering	ΔV (m/s)	[baseline, x2, x4]	9	0	3	9	0	0	0	0
			s/c servicing interface	[none, tugable, refuel, ORU]	9	0	1	1	0	0	0	0
		ground receiver maneuverability	mobile receiver	[yes, no]	0	0	0	0	3	0	0	3
Type II	hardness	radiation-hardened electronics	hardening	[yes, no]	0	3	9	3	0	0	0	0
		bumper shielding	shield thickness (cm)	[0, 0.1, 0.3]	0	0	0	9	0	0	0	0
	redundancy	duplicate critical s/c functions	bus redundancy	[yes, no]	0	1	9	9	0	0	0	0
		on-orbit satellite spares	extra s/c per orbital plan	[0, 1, 2]	0	1	3	9	0	0	0	0
		multiple ground receivers	ground infrastructure level	[AFSCN, AFSCN+]	0	0	0	0	3	0	0	9
	margin	over-design power generation	peak transmit power (kW)	[baseline, +5%, +10%]	0	0	0	3	9	9	0	0
		over-design link budget	assumed signal loss (dB)	[0, 3, 6]	0	0	0	0	9	0	0	0
		over-design propulsion system	ΔV (m/s)	[baseline, x2, x4]	3	0	3	0	3	9	0	0
		excess on-board data storage	s/c data capacity (gbits)	[baseline, x2, x3]	0	0	0	0	0	0	3	3
		excess constellation capacity	number of satellites	[5, 10, 20]	0	1	3	9	0	0	0	0
	heterogeneity	interface with airborne assets	tactical downlink	[yes, no]	3	3	3	3	3	3	3	3
		multiple communication paths	ground communication	[ground station, +relay]	0	0	1	1	9	0	9	3
			tactical downlink	[yes, no]	0	0	1	1	9	0	9	9
	distribution	spatial separation of spacecraft	orbital altitude (km)	[800, 1200, 1500]	1	1	3	3	0	9	0	0
		spatial separation of s/c orbits	number of planes	[5, 10]	0	0	3	9	0	1	0	1
	failure mode reduction	reduce s/c complexity	telemetry	[hardwired, programmable]	0	0	9	0	0	0	0	0
	fail-safe	autonomous operations	autonomous control	[yes, no]	0	0	0	0	3	0	3	3
	evolution	flexible sensing operations	antenna type	[parabolic, AESA]	0	0	0	0	3	9	0	0
			radar bandwidth (GHz)	[0.5, 1, 2]	0	0	0	0	9	3	0	0
		retraction of s/c appendages	reconfigurable	[yes, no]	0	0	9	3	0	0	0	0
	containment	s/c fault monitoring and response	autonomous control	[yes, no]	0	1	3	1	0	0	0	0
T III	replacement	rapid reconstitution	constellation option	[none, long-lead, spares]	0	1	3	9	0	0	0	0
	repair	on-orbit-servicing	s/c servicing interface	[none, tugable, refuel, ORU]	9	1	3	3	0	9	0	0

The fourth step is to parameterize the survivable concepts by specifying design variables (*i.e.*, translating column two to column three in Table 4). 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. The design variables operationalize each concept for subsequent tradespace exploration. Each design variable includes units and an enumerated range of values for analysis (column four). 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.[3]

[3] 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 are selected that will drive the dependent variables across a large range. In the sampling phase, a subset of values in the enumerated

For example, the concept of over-designing the satellite communications link budget (from the Type II design principle of margin) is specified by the design variable, assumed signal loss, to be evaluated at the values of 0, 3, and 6 dB. 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.

The fifth step is to assess the degree of impact of each survivability design variable on each disturbance type. In a process analogous to the design value mapping matrix (where the ability of candidate design variables to drive system attributes is assessed), the ability of the candidate survivability design variables to mitigate the impact of system disturbances is now assessed. As illustrated in the disturbance columns in Table 4, the number (*i.e.*, 0, 1, 3, or 9) indicates the level of impact that the design survivable has on mitigating a given disturbance based on the use context provided by the particular concept enhancement. For example, the design variable of assumed signal loss will reduce the impact of signal attenuation but will not directly mitigate any of the other disturbances.

The sixth step is 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. For example, providing the satellite with a servicing interface (*i.e.*, docking port) may enable utilization of an orbital transfer vehicle for enhanced maneuverability as well a robotic servicing vehicle for on-orbit repair of damaged components. In consolidating duplicate design variable rows in the survivability design matrix, the maximum mitigating impact score for each disturbance is kept. The design variables and disturbances columns in Table 5 illustrate the output of this step for the satellite radar system.

rage is selected for inclusion in the tradespace analysis. The sampling phase is necessary to efficiently utilize finite computing resources.

Table 5. Selecting Survivability Enhancement Features for Inclusion in Design Space

	survivability design principles																disturbances									
	Type I						Type II								Type III											
design variables (units)	prevention	mobility	concealment	deterrence	preemption	avoidance	hardness	redundancy	margin	heterogeneity	distribution	failure mode reduction	fail-safe	evolution	containment	replacement	repair	atmospheric drag fluctuations	arc discharging	high-flux radiation	micrometeorites / debris	signal attenuation	change in target characteristics	loss of relay backbone	loss of ground node	type	impact
tactical downlink										X								3	3	3	3	9	3	9	3	baseline	**162**
communications downlink										X								0	0	1	1	9	0	9	3	baseline	**116**
peak transmit power (kW)									X									0	0	0	3	9	9	0	0	baseline	**102**
antenna area (m^2)	X																	9	0	3	9	0	0	0	0	baseline	**84**
number of planes											X							0	0	3	9	0	1	0	1	baseline	**81**
ΔV (m/s)						X			X									9	0	3	1	3	9	0	0	baseline	**79**
constellation spares																X		0	1	3	9	0	0	0	0		**78**
number of satellites									X									0	1	3	9	0	0	0	0	baseline	**78**
orbital altitude (km)											X							1	1	3	3	0	9	0	0	baseline	**73**
shield thickness (cm)							X											0	0	0	9	0	0	0	0		**63**
autonomous control													X		X			0	1	3	1	3	0	3	3		**61**
bus redundancy								X										0	1	9	3	0	0	0	0		**60**
s/c servicing interface						X											X	9	1	3	3	0	3	0	0		**57**
radar bandwidth (GHz)														X				0	0	0	0	9	3	0	0	baseline	**57**
reconfigurable														X				0	0	9	3	0	0	0	0		**57**
hardening							X											0	3	9	1	0	0	0	0		**52**
antenna type														X				0	0	0	0	3	9	0	0		**51**
extra s/c per orbital plan								X										0	1	3	3	0	3	0	0		**48**
assumed signal loss (dB)									X									0	0	0	0	9	0	0	0		**45**
telemetry												X						0	0	9	0	0	0	0	0		**36**
ground infrastructure level								X										0	0	0	0	3	0	0	9		**33**
s/c data capacity (gbits)									X									0	0	0	0	0	0	3	3		**24**
mobile receiver						X												0	0	0	0	3	0	0	3		**21**
															weight			1	3	4	7	5	4	6	2		

The seventh through tenth steps of applying the survivability design principles to the concept generation phase of MATE involve filtering the expanded number of design variables and selecting a small number for inclusion in the tradespace. In the seventh step, the coverage of the consolidated set of design variables across the seventeen design principles is examined (Table 5). 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.

In the eighth step, the mitigating impact of each consolidated design variable across the set of disturbances is aggregated using a linear-weighted sum. In this ninth step, this aggregate impact score is used to order the consolidated design variables for consideration. The tenth and final step is to down-select survivability design variables for inclusion in the expanded design-space. As illustrated in the "type" column in Table 5, many survivability design variables are already inherent in the baseline tradespace. In determining which new design variables to include, several considerations are recommended: 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" (*e.g.*, moving the binary

survivability design variable of autonomy to the constant variable list). Given these factors, two additional survivability design variables were selected for inclusion in the preliminary design vector for satellite radar: satellite shielding and constellation spares for rapid reconstitution.

Model System Performance and Evaluate Tradespace

The last phase of MATE, design alternative evaluation, involves the development of physics-based performance models to predict the lifecycle cost and utility of the designs under consideration. To assess the sampling of the design space, parametric computer models are developed to transform each design vector into attribute values against which utility functions can be applied. The broad, front-end evaluation of thousands of design alternatives on a common, quantitative basis provides decision makers a prescriptive framework for selecting designs to carry forward for more detailed analysis (Figure 1).

To incorporate survivability considerations into the design alternative evaluation phase, the MATE analysis must be extended beyond deterministic calculations of lifecycle cost and the utility provided by the system at beginning-of-life. In particular, a dynamic state model of systems operating across disturbance environment is developed, evaluating the stochastic performance of design alternatives (*i.e.*, utility trajectories over time) as a function of their survivability enhancement features. As observed in the utility trajectories in Figure 2, the outcome of a particular run of the dynamic state model is probabilistic in nature. Therefore, a Monte Carlo analysis is performed over multiple utility trajectories for each design and statistical measures of survivability are applied to the simulations runs.

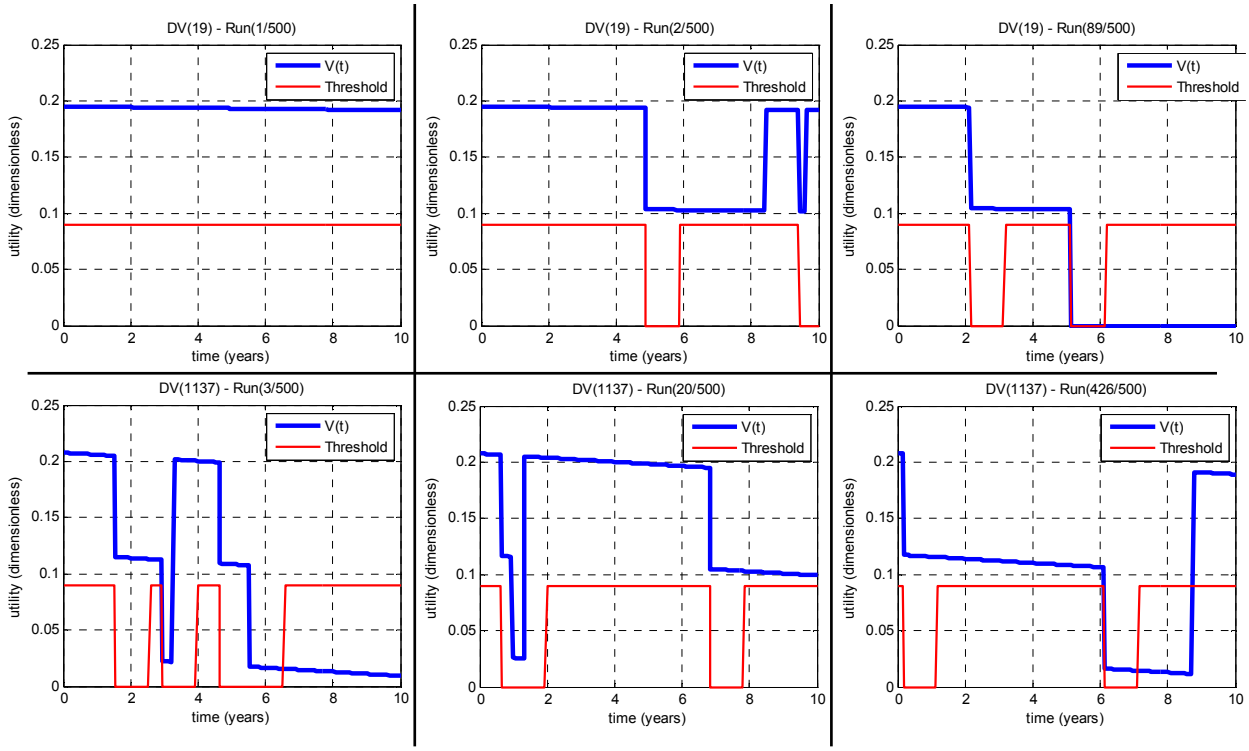

Figure 2. Samples from Two Distributions of Utility Trajectories (Richards et al. 2008c)

Finally, the deterministic cost-utility tradespace is integrated with summary statistics of the utility trajectories in a survivability tradespace (Richards, Ross et al. 2008c). Rather than judging the value of design based upon maximizing utility at cost, survivability tradespaces are used to discover designs which are both cost-effective and robust to environmental disturbances.

Discussion

The process described above for applying the survivability design principles within Multi-Attribute Tradespace Exploration provides a structured approach for generating concepts that may be better equipped to operate in the presence of environmental disturbances. The intent of the process is twofold: (1) to augment the creativity of system designers by ensuring consideration of a broad tradespace of design alternatives and (2) to quickly screen and prioritize a large number of candidate design variables before proceeding to the design evaluation phase of MATE. This latter task is necessary to prevent the design-space from growing too large. In applying the design principles to a MATE study of satellite radar, many latent survivability trades were found within the baseline set of design variables. The survivability design matrices introduced in this paper provide an explicit means for recognizing these latent trades, informing utility-survivability interactions and the selection of baseline design variable enumeration ranges. More importantly, the survivability design matrices also identify emergent design variables that may warrant inclusion in the trade study.

In applying the survivability design principles within MATE, several implementation issues arose. First, in enumerating potential system disturbances, it is necessary to account for interactions among disturbances which may impact the system in nonlinear ways. Second, completing the design matrices requires judgment and experience. In mapping system design variables to desired outcomes (whether to drive attributes or mitigate disturbances), each matrix is effectively a qualitative model that must be completed by a subject matter expert. Third, in the design evaluation phase of MATE, modeling the impact of survivability enhancement features that rely on behavioral design principles (rather than structural) requires implicit assumptions to be made regarding the system's concept-of-operations. These operational design principles must be reflected in the modeling effort.

Empirical testing of the validity of the design principle framework involved a bottom-up analysis of tracing survivability features on existing systems to functional strategies. The application of the design principles here to satellite radar demonstrates that the principles may be used from the top-down to inform the concept generation phase of trade studies. A large number of survivable concepts were rapidly brainstormed and parameterized by consulting the design principles (steps three and four). While considerably more time was involved in anticipating how each design variable will mitigate the disturbances (step five), such effort is critical for down-selecting among the design variables, ensuring that the important survivability trades are incorporated into subsequent modeling activities. Incorporating survivability considerations into the concept generation phase stands in contrast to most survivability analysis methodologies which focus on whether to incorporate a particular design feature (*e.g.,* level of hardening on satellites) after a baseline system concept has been established. By incorporating survivability considerations before a set of design vectors has been defined, the methodology introduced in this paper allows architectural trades (*e.g.*, constellation structure) to be made in concert with these system-level trades.

The initial application of the design principles to tradespace exploration in this paper uncovered many areas for future work. For example, future studies might examine the impact of intelligent disturbances environments on the proposed approach as well as experiment with different representations in mapping design principles to concepts and design variables (*e.g.*, network diagram). There are also opportunities to extend the scope of the analysis beyond the system-level. Given that critical infrastructures may be increasingly characterized as systems-of-systems, survivability methods should extend in scope to accommodate applications of the heterogeneity design principle at the architecture level. In the context of concept generation within trade studies, such an accommodation would mean considering portfolios of systems with each system specified as a unique design matrix. Finally, while the present work presents an outline of the application of the survivability design principles to concept generation, future work should provide detailed documentation of an end-to-end tradespace exploration methodology for survivability through the design evaluation phase.

Conclusion

The operational environment of engineering systems is increasingly characterized by disturbances which may asymmetrically degrade performance, particularly for systems with networked structures. The approach introduced in this paper for applying the seventeen survivability design principles to concept generation provides a structured framework for incorporating survivability considerations into front-end system analysis. As demonstrated in the Multi-Attribute Tradespace Exploration study of a satellite radar system, 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.

Acknowledgements

The authors thank Andrew Long and Nirav Shah for their constructive feedback. 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

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*.

Ahn, J., S. Lee and J. Kim (2002). "A Robust Approach to Pre-Concept Design of UCAV Considering Survivability." *9th AIAA Symposium on Multidisciplinary Analysis and Optimization*, Atlanta, GA.

Al-Noman, A. (1998). "Analysis and Evaluation of Survivability of Various Configured Communication Networks." *International Journal of Communication Systems,* 11: 305-310.

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.

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

Ball, R. and D. Atkinson (2006). "Designing for Survivability." *Aircraft Survivability,* Fall 2006: 26-29.

Baran, P. (1964). On Distributed Communications. Santa Monica, CA, RAND Corporation.

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.

Bennett, B. (1980). "How to Assess the Survivability of U.S. ICBMs." *RAND Corporation*. Santa Monica, CA.

Blanchard, B. and W. Fabrycky (2006). Systems Engineering and Analysis. Upper Saddle River, Prentice Hall.

Canavan, G. (1989). "Survivability of Space Assets in the Long-Term." *Los Alamos National Laboratory*. DE89-006563, New Mexico.

Canavan, G. (1997). "Costs of Strikes Between Vulnerable Missile Forces." *Los Alamos National Laboratory*. LA-UR-97-663, New Mexico.

Canavan, G. and E. Teller (1990). "Strategic Defence for the 1990s." *Nature*, 19 April 1990, 699-702.

Catchpole, K., M. de Leval, A. McEwan, N. Pigott, M. Elliott, A. McQuillan, C. MacDonald and A. Goldmans (2007). "Patient Handover from Surgery to Intensive Care: Using Formula 1 Pit-Stop and Aviation Models to Improve Safety and Quality." *Pediatric Anesthesia,* 17(5): 470-478.

DoD (2002). "DoD Regulation 5000.2-R - Mandatory Procedures for Major Defense Acquisitions Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs." 5 April 2002.

Ellison, R., D. Fisher, R. Linger, H. Lipson, T. Longstaff and N. Mead (1999). "Survivable Network Systems: An Emerging Discipline." *Carnegie Mellon Software Engineering Institute*.

Heydorn, R. and J. Railsback (1999). Chapter 8: Safety of Crewed Spaceflight. Human Spaceflight Mission Analysis and Design. W. Larson and L. Pranke. New York, McGraw-Hill.

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

Howard, M. (1993). "First-Order Models for Satellite Survivability Optimization." *Journal of Guidance, Control, and Dynamics,* 16(3): 462-469.

Jeffcoat, D. (2003). "The Survivability Versus Quantity Trade-Off for Unmanned Aerial Vehicles." *2nd AIAA Unmanned Systems Conference*, San Diego, CA.

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

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

Lin, T. (2003). "Development of U.S. Air Force Intercontinental Ballistic Missile Weapon Systems." *Journal of Spacecraft and Rockets,* 40(4): 491-509.

Nakano, T. and T. Suda (2007). "Applying Biological Principles to Designs of Network Services." *Applied Soft Computing,* 7: 870-878.

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

Nordin, P. and M. Kong (1999). Chapter 8.2 Hardness and Survivability Requirements. Space Mission Analysis and Design. El Segundo, Microcosm Press.

Northrop, L., P. Feiler, R. Gabriel, J. Goodenough, R. Linger, T. Longstaff, R. Kazman, M. Klein, D. Schmidt, K. Sullivan and K. Wallnau (2006). "Ultra-Large-Scale Systems: The Software Challenge of the Future." *Software Engineering Institute.* Pittsburgh, PA.

Paterson, J. (1999). "Overview of Low Observable Technology and Its Effects on Combat Aircraft Survivability." *Journal of Aircraft,* 36(2): 380-388.

Perrow, C. (2007). The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters. Princeton, Princeton University Press.

Pisacane, V. (2008). The Space Environment and Its Effects on Space Systems. Reston, American Institute of Aeronautics & Astronautics.

Richards, M., A. Ross, D. Hastings and D. Rhodes (2007). "Design Principles for Survivable System Architecture." *1st IEEE Systems Conference*, Honolulu, HI.

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

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

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

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.

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.

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."

Shaw, G., D. Miller and D. Hastings (2001). "Development of the Quantitative Generalized Information Network Analysis Methodology for Satellite Systems." *Journal of Spacecraft and Rockets,* 38(2): 257-269.

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

Throndson, L. (1982). "Combat Survivability with Advanced Aircraft Propulsion Development." *Journal of Aircraft,* 19(11): 915-920.

Tribble, A. (2003). The Space Environment: Implications for Spacecraft Design. Princeton, Princeton University Press.

Williamsen, J., K. Blacklock, H. Evans and T. Guay (1999). "Quantifying and Reducing International Space Station Vulnerability Following Orbital Debris Penetration." *Journal of Spacecraft and Rockets,* 36(1): 133-141.

Biographies

Matthew Richards is a Ph.D. candidate in the Engineering Systems Division (ESD) at the Massachusetts Institute of Technology (MIT). As a research assistant for MIT's Systems Engineering Advancement Research Initiative (SEAri), his current research is focused on survivable system architecture, value-robust design, and tradespace exploration of complex systems. Matt's work experience includes Mars rover mission design at the Jet Propulsion Laboratory (JPL) and systems engineering support on two autonomous vehicle programs for the Defense Advanced Research Projects Agency. From MIT, Matt has B.S. and M.S. degrees in Aerospace Engineering (2004, 2006) and an M.S. degree in Technology and Policy (2006).

Adam Ross is a Research Scientist in ESD and a co-founder of SEAri. His research focuses on managing unarticulated value, designing for changeability, and dynamic tradespace exploration for complex systems. Dr. Ross received his Ph.D. from ESD in June 2006 and has published papers in the area of space systems design. He has work experience with government, industry, and academia including NASA Goddard; JPL; the Smithsonian Astrophysical Observatory; Boeing Satellite Systems; MIT; and Harvard and Florida State Universities; performing both science and engineering research.

Daniel Hastings is a Professor of Aeronautics and Astronautics and Engineering Systems at MIT. Dr. Hastings has taught courses and seminars in plasma physics, rocket propulsion, advanced space power and propulsion systems, aerospace policy, technology and policy, and space systems engineering. He served as chief scientist to the U.S. Air Force from 1997 to 1999, as director of MIT's Engineering Systems Division from 2004 to 2005, and is a former chair of the Air Force Scientific Advisory Board. Dr. Hastings was elected a Fellow of the International Council on Systems Engineering (INCOSE) in June 2007.

Donna Rhodes is the director of SEAri and a Senior Lecturer in Engineering Systems at MIT. Her research interests are focused on systems engineering, systems management, and enterprise architecting. Dr. Rhodes has 20 years of experience in the aerospace, defense systems, systems integration, and commercial product industries. Prior to joining MIT, she held senior level management positions at IBM Federal Systems, Lockheed Martin, and Lucent Technologies in the areas of systems engineering and enterprise transformation. Dr. Rhodes is a Past-President and Fellow of INCOSE, and the 2005 recipient of the INCOSE Founders Award.