MULTI-ATTRIBUTE TRADESPACE EXPLORATION FOR SURVIVABILITY

by

Matthew G. Richards

S.B., Aeronautics and Astronautics, Massachusetts Institute of Technology, 2004
S.M., Technology and Policy, Massachusetts Institute of Technology, 2006
S.M., Aeronautics and Astronautics, Massachusetts Institute of Technology, 2006

Submitted to the Engineering Systems Division (ESD)
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in ENGINEERING SYSTEMS
at the
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
June 2009

Signature of Author..
Engineering Systems Division
April 9, 2009

Certified by..
Daniel E. Hastings, Professor of Aeronautics and Astronautics and Engineering Systems
Dean for Undergraduate Education
Thesis Supervisor

Certified by..
Donna H. Rhodes, Senior Lecturer of Engineering Systems
Thesis Committee Member

Certified by..
Adam M. Ross, Research Scientist of Engineering Systems
Thesis Committee Member

Certified by..
Annalisa L. Weigel, Assistant Professor of Aeronautics and Astronautics and Engineering Systems
Thesis Committee Member

Accepted by..
Nancy G. Leveson, Professor of Aeronautics and Astronautics and Engineering Systems
Chair, ESD Education Committee

MULTI-ATTRIBUTE TRADESPACE EXPLORATION FOR SURVIVABILITY

by
Matthew G. Richards

Submitted to the Engineering Systems Division on April 9, 2009, in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Engineering Systems.

Abstract

Survivability is the ability of a system to minimize the impact of a finite-duration disturbance on value delivery (*i.e.*, stakeholder benefit at cost), achieved through (1) the reduction of the likelihood or magnitude of a disturbance, (2) the satisfaction of a minimally acceptable level of value delivery during and after a disturbance, and/or (3) a timely recovery. Traditionally specified as a requirement in military systems, survivability is an increasingly important consideration for all engineering systems given the proliferation of natural and artificial threats. Although survivability is an emergent system property that arises from interactions between a system and its environment, conventional approaches to survivability engineering are reductionist in nature. Furthermore, current methods neither accommodate dynamic threat environments nor facilitate stakeholder communication for conducting trade-offs among system lifecycle cost, mission utility, and operational survivability.

Multi-Attribute Tradespace Exploration (MATE) for Survivability is introduced as a system analysis methodology to improve the generation and evaluation of survivable alternatives during conceptual design. MATE for Survivability applies decision theory to the parametric modeling of thousands of design alternatives across representative distributions of disturbance environments. To improve the generation of survivable alternatives, seventeen empirically-validated survivability design principles are introduced. The general set of design principles allows the consideration of structural and behavioral strategies for mitigating the impact of disturbances over the lifecycle of a given encounter. To improve the evaluation of survivability, value-based metrics are introduced for the assessment of survivability as a dynamic, continuous, and path-dependent system property. Two of these metrics, time-weighted average utility loss and threshold availability, are used to evaluate survivability based on the relationship between stochastic utility trajectories of system state and stakeholder expectations across nominal and perturbed environments. Finally, the survivability "tear(drop)" tradespace is introduced to enable the identification of inherently survivable architectures that efficiently balance performance metrics of cost, utility, and survivability.

The internal validity and prescriptive value of the design principles, metrics, and tradespaces comprising MATE for Survivability are established through applications to the designs of an orbital transfer vehicle and a satellite radar system.

Thesis Supervisor: Daniel E. Hastings
Title: Professor of Engineering Systems and Aeronautics and Astronautics

Acknowledgements

Since arriving nine years ago as an undergraduate, my journey through MIT has been a blessing, and I leave with a tremendous sense of gratitude to those special individuals who made my journey possible.

I thank my advisor, **Prof. Daniel Hastings**, for the creative freedom to pursue this research topic, for guiding my development as a deep thinker, and for always keeping my research grounded in applications to real engineering systems. His technical mastery of spacecraft-environmental interactions, generosity with his time, and uncommon ability to inspire allowed me to maximize my potential in graduate school. I am extremely fortunate to be the beneficiary of his sound advice, and the principles he instilled in my intellect and character will guide me through future challenges.

As both the co-advisor of my Master's research and a member of my doctoral committee, **Dr. Donna Rhodes** pushed me to reach beyond my aerospace roots and explore the applicability of my theories and methods to the larger systems engineering community. Her feedback, encouragement, and thoughtfulness sustained me personally and professionally. I am also indebted to her for establishing the Systems Engineering Advancement Research Initiative (SEAri), which provided me a community for intellectual "scrubbings," access to industry viewpoints, and a host of collaborative research opportunities

Through graduate school, I sought to model my attitude, self-discipline, and goals around the superior example set by **Dr. Adam Ross**. In addition to following his foundational work on Multi-Attribute Tradespace Exploration and system changeability, many of the ideas of this thesis emerged with his creative inspiration. I could not ask for a more supportive committee member or friend. Our weekly research meetings will be sorely missed.

As a committee member, instructor, and professional mentor, **Prof. Annalisa Weigel** has broadened and enriched my perspectives of the aerospace industry. I am particularly grateful for the research opportunities she has afforded me within her own research group in the areas of space policy, innovation management, and fractionated spacecraft. I will always remember the wisdom and kindness she has shown me as an advisor over the past five years.

I thank the students of SEAri for their friendship, encouragement, and support as I navigated through the challenges of the Ph.D. program. I especially thank **David Broniatowski** for our spirited debates; **Luke Cropsey** for his leadership; **Greg O'Neill** for his inspiring work ethic; **Nirav Shah** for his selfless, invaluable help; and **Jason Bartolomei**, **Deb Chattopadhyay**, **Spencer Lewis**, **Kevin Liu**, **Tsoline Mikaelian**, **Julia Nickel**, **Chris Roberts**, **Dave Stein**, **Jennifer Wilds**, and **Lauren Viscito**. I also thank **Mr. Andrew Long**, **Dr. Hugh McManus**, and **Dr. Ricardo Valerdi** for enriching the SEAri community.

I am extremely grateful to MIT's Program on Emerging Technologies (PoET) for the National Science Foundation traineeship that supported me through three years of doctoral education. The collaborative research opportunities within PoET made my ESD experience truly interdisciplinary. I particularly thank **Prof. Dava Newman**, **Prof. Ken Oye**, **Prof. Merritt Roe**

Smith, Dr. David Clark, **Dr. Frank Field**, and **Dr. Larry McCray** for their leadership; and fellow PoET students **Kieran Downes**, **Katherine Dykes**, **Lisa Messeri**, **Matthew Silver**, **Kate Steel**, **Chintan Vaishnav**, and **Rachel Wellhausen** for the opportunity to work together on a variety of projects.

It would be impossible to acknowledge all of the faculty, staff, and students who have enriched my MIT experience. I especially thank **Prof. Oli de Weck**, **Prof. Daniel Frey**, **Prof. Debbie Nightingale**, **Prof. Chris Magee**, **Prof. Dave Miller**, **Prof. Joel Moses**, **Prof. Susan Silbey**, **Prof. Joe Sussman,** and **Dr. Daniel Whitney** for their teaching, research insights, and professional mentorship; **Fran Marrone** and **Marie Stuppard**; fellow graduate students **Mark Avnet**, **Yves Boussemart**, **Michel Cardin**, **Lucy Cohan**, **Phech Colatat**, **Heidi Davidz**, **Mark Davis**, **Dietrich Falkenthal**, **Dan Gillespie**, **Erica Gralla**, **Kenfield Griffith**, **Rhonda Jordan**, **Caroline Lamb**, **Joe Laracy**, **Chris Lawson**, **Dan Livengood**, **Pedzi Makumbe**, **Doug Matty**, **Jorge Oliveira**, **Brandon Owens**, **Roberto Perez-Franco**, **Sameera Ponda**, **Sid Rupani**, **Nandan Sudarsanam**, **Zoe Szajnfarber**, and **Danielle Wood**; Kappa Sigma brothers **Cameron Bass**, **Larry Colagiovanni**, **Sanjay Divakaran**, **Arturo Hinojosa**, **Mike Menard**, **Sam Prentice**, **Mike Ramos**, **Cliff Roscow**, **Jon Schechter**, and **Jake Simson**; and alumni **Atif Qadir** and **Phil Springmann**.

I have also been supported by a community of friends and colleagues outside of MIT. I am especially grateful to **Mr. Eric Bright**, **Mr. Jon Estridge**, **Mr. Rich Fink**, **Mr. Scott Jackson**, **Dr. Cyrus Jilla**, **Mrs. Amy Malarkey**, **Mr. Rob McHenry**, **Mrs. Michelle Menza**, **Ms. Darlene Minick**, **Mr. Ross Perkins**, **Dr. Rob Perrons**, **Mr. Dave Pinson**, **Dr. Michaela Shoop**, **Dr. Steve Shoop**, the late **Mr. John Wirsbinski**, **Mr. Jeff Vickers**, and **Mr. Eric Viglione**.

I thank **Dr. Pete Rustan** for his thoughtful mentorship, contagious energy and enthusiasm, and visionary approaches to solving technical challenges.

Since seeking his advice regarding my choice for higher education, I have been blessed by the strong and positive mentoring of **Dr. Albert Wheelon**. His accomplishments in government and industry provide a sustaining source of inspiration.

I am indebted to my parents, **Rev. Greg Richards** and **Mrs. Debbie Richards**, for their love, encouragement, and support. I thank them for their sacrifices in making the education of their two sons their highest priority, and for the pride, determination, and confidence that they have instilled in me. I also thank my brother **Michael Richards** for the grit and fortitude that he has displayed in his own educational journey. He provides a stirring example for us all.

My higher education is only one of two treasures that I have received while at MIT. Fellow student and fiancée, **Amy Marshall,** has been steadfast supporter, friend, and partner through three challenging years. I thank her for the grace, joy, and spirit that she brings to my life.

Table of Contents

List of Figures

List of Tables

Acronyms

AESA	active electronically scanned array
AFSCN	Air Force Satellite Control Network
AISR	airborne intelligence, surveillance, and reconnaissance
AMTI	air-moving target identification
AoA	analysis-of-alternatives
ASAT	anti-satellite
AWACS	Airborne Warning and Control System
BMD	ballistic missile defense
BOL	beginning-of-life
CEO	chief executive officer
CONOPS	concept-of-operations
DARPA	Defense Advanced Research Projects Agency
DIA	Defense Intelligence Agency
DoD	Department of Defense
DV	design vector
EMP	electromagnetic pulse
EOL	end-of-life
ESD	Engineering Systems Division (MIT)
FTA	fault tree analysis
FMEA	failure modes and effects analysis
FoS	family-of-systems
GEO	geostationary orbit
GINA	Generalized Information Network Analysis
GMTI	ground-moving target identification
HOT	Highly Optimized Tolerance
ICBM	inter-continental ballistic missile
ILSP	integrated logistics support plan
IOC	initial operational capability
ISS	International Space Station
JSTARS	Joint Surveillance Target Attack Radar System
LDEF	Long-Duration Exposure Facility
LEO	low Earth orbit
MATE	Multi-Attribute Tradespace Exploration
MATE-CON	Multi-Attribute Tradespace Exploration with Concurrent Design
MAUT	multi-attribute utility theory
MDV	minimum detectable velocity
MIT	Massachusetts Institute of Technology
MNS	mission needs statement
NCCS	nuclear command and control system
NORAD	North American Aerospace Defense Command
NSS	national security space
ORD	operational requirements document
ORS	operationally responsive space
PRA	probabilistic risk assessment

QALY	quality-adjusted life year
radar	radio detection and ranging
RCS	radar cross-section
RSC	Responsive Systems Comparison method
SAR	synthetic aperture radar
SATCOM	satellite communications
SEAri	Systems Engineering Advancement Research Initiative
SoS	systems-of-systems
SR	satellite radar
SSA	space situational awareness
SSN	space surveillance network
STAR	system threat assessment report
TEMP	test and evaluation master plan
TRL	technology readiness level
UAV	uninhabited aerial vehicle
USC	University of Southern California
WGS	Wideband Global SATCOM System

1. Introduction

The operational environment of engineering systems is increasingly characterized by disturbances which may asymmetrically degrade performance, particularly for interdependent infrastructure systems. In recent years, hostile actors have preyed upon networked infrastructures, whether physically, electrically, or economically.

- Businesses incurred an estimated $5.5 billion in damages from the 2000 ILOVEYOU Internet virus which generated thousands and thousands of emails (an assault on Internet links by overwhelming limited bandwidth) and overwrote important files on servers and workstations (an assault on Internet nodes).

- The tragic events of September 11, 2001, that injured and killed thousands of people, may also be viewed as a psychological attack on our interdependent economy, with four physical disturbances causing a $1.2 trillion loss in the valuation of U.S. stocks in the week following the tragedy (Kean et al. 2004).

Engineering systems are also vulnerable to natural threats arising from the environment.

- The outage of a generating plant in Parma, OH, in 2003, triggered a massive power outage across the Northeast, affecting 40 million people in eight states (Abraham and Efford 2004).

- Hurricane Katrina breached the levees of New Orleans, subsequently flooding 80% of the city—costing 2,000 lives and over $80 billion in damages (Knabb, Rhome and Brown 2005).

In response to these artificial (*i.e.*, human-directed) and natural disturbances, numerous studies and several government and academic research initiatives have been launched.

- Following the terrorist attacks of September 11th, hundreds of national studies have identified vulnerabilities in critical economic infrastructures—including information, transportation, energy, retail, manufacturing, and finance—which reside in the private sector and are largely not hardened. For example, the Rumsfeld Commission to Assess U.S. National Security Space Management and Organization surveyed satellite vulnerabilities to various hostile acts (*e.g.*, denial and deception, interference, jamming, microsatellite attacks, nuclear detonation) and found that the impact of such surprise attacks could constitute a "Pearl Harbor" in space. Risks are further exacerbated by reliance on unhardened commercial systems and inadequate space situational awareness (Rumsfeld et al. 2001).

- Recent research at the Massachusetts Institute of Technology (MIT) has focused on corporate security and resilience with an emphasis on creating enterprises with supply chains robust to high-impact disturbances. For example, the pressure to achieve cost efficiencies has led to the "leaning" of global supply chains that are now extremely fragile to disruptions (Sheffi 2005). Empirical evidence indicates the need for balance between security, redundancy, and short-term profits.

- In October 2006 at the University of Southern California's (USC) Center for Systems and Software Engineering, stakeholders from commercial organizations (*e.g.*, Motorola, Bosch), defense companies (Lockheed Martin, Northrop Grumman, and Boeing), and academia (USC and MIT) identified resilience engineering as the top priority for system of systems architecting (Axelband et al. 2007). An extension of the traditional fields of reliability engineering and safety management, resilience engineering incorporates the principles of the Santa Fe Institute and Highly Optimized Tolerance (HOT) (Carlson and Doyle 2000), positing that safety emerges from an aggregate of system components, subsystems, software, organizations, human behaviors, and interactions among them. To be resilient, systems must not only be reliable but must also be able to recover from disturbances through the design of proactive organizations and processes (Hollnagel, Woods and Leveson 2006).

While related in terms of the common objective of protecting critical societal infrastructure, methodological approaches towards mitigating disturbances have evolved almost exclusively within the context of individual engineering disciplines and infrastructure domains. Given its development within MIT's interdisciplinary Engineering Systems Division (ESD), this dissertation aims to consolidate knowledge on survivability residing across numerous disciplines and application areas. This introductory chapter provides context to the research in Section 1.1 through a brief overview of ESD and the value-based design methods underlying the research. Section 1.2 summarizes the motivation for enhancing survivability analysis through a detailed examination of protection concerns for one critical infrastructure: satellite design and operation. Section 1.3 introduces the research questions, followed by Section 1.4 which discusses the four-part research approach. Section 1.5 concludes the chapter with an overview of the thesis structure.

1.1. Context

1.1.1. MIT Engineering Systems Division

The MIT Engineering Systems Division was founded in 1998 to establish an interdisciplinary field of study for the engineering of large-scale, complex, socio-technical systems characterized by significant enterprise level interactions (Moses 2004; Roos 2004). Whereas systems engineering may be defined as "the art and science of developing an operable system capable of meeting requirements within imposed constraints" (Griffin 2007), engineering systems embraces the design (*i.e.*, the "art") and analysis (*i.e.*, the "science") of artifacts while also incorporating the contextual social and enterprise factors (Rhodes and Hastings 2004). As such, understanding and improving engineering systems requires a holistic perspective, integrating domains that are normally treated as separate from traditional engineering. Engineering systems research is distinguished by particular emphases on (1) interdisciplinary methods which span technology, management, and policy; (2) temporal system properties, commonly referred to as the "-ilities"; (3) the interconnectedness of product systems with the enterprises that develop and sustain them; and (4) value stream complexities arising from stakeholder heterogeneity.

The scope of engineering systems research spans operations research and systems analysis; systems engineering, architecting, and product development; engineering management; and technology and policy (Hastings 2004). This thesis, however, focuses on systems engineering, architecting and analysis through advancing value-based design methods. A system architecture is an integrated description of the operations, components, and technical standards of a system, consisting of a functional decomposition (from originating requirements) in the behavioral domain and an allocation of functions to components in the physical domain, all occurring within an environmental context (Crawley et al. 2004; Richards 2006). A standard definition of architecture used by the Department of Defense (2003a) is “the structure of components, their relationships, and the principles and guidelines governing their design and evolution over time.” The process of creating and building architectures is referred to as systems architecting and concerns itself most with system conceptualization, objective definition, and certification for use (Maier and Rechtin 2002). Accordingly, systems architecting “strives for fit, balance, and compromise among the tensions of client needs and resources, technology, and multiple stakeholder interests” (Maier and Rechtin 2002).

1.1.2. Value-Based Conceptual Design

Within systems engineering, the research focuses on the application of value-based methods to conceptual design. Value may be defined generally as benefit at cost. As a subjective measure of benefit from a bundle of consequences that is specified by a stakeholder, value provides a fundamental metric for relating system properties to desired stakeholder outcomes (Keeney 1992). Empirical evidence suggests that the lifecycle value delivered by systems is primarily determined at the beginning of development programs (Figure 1-1), highlighting the criticality of good decision-making during conceptual design.

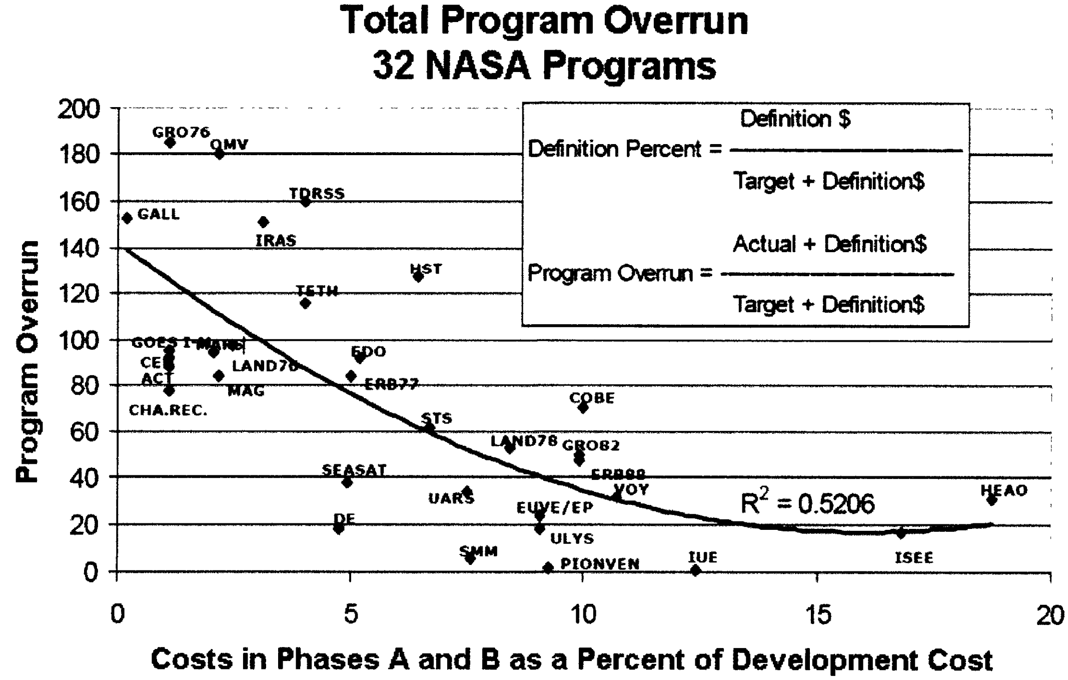


Figure 1-1. Critical Front-End in System Development (Gruhl 1992)

As illustrated in Figure 1-2, conceptual design includes both concept development (*i.e.*, identification of stakeholders, enumeration and evaluation of design alternatives, and selection of one or more concepts for further development) and system-level design (*i.e.*, definition of the architecture, including subsystem decompositions and functional specifications) (Ulrich and Eppinger 2004). Taking the value-centric perspective during conceptual design empowers decision-makers[1] rigorously to evaluate and to compare different system concepts in the technical domain (*e.g.*, geosynchronous satellite vis-à-vis low-Earth orbit satellite constellation for a communications mission) using a unifying set of attributes in the value domain (*e.g.*, signal isolation, information rate, information integrity, and data availability) (Shaw, Miller and Hastings 2001).

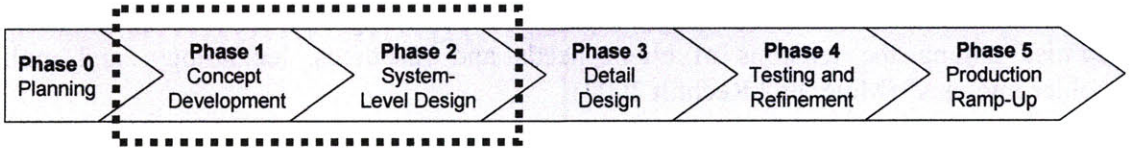


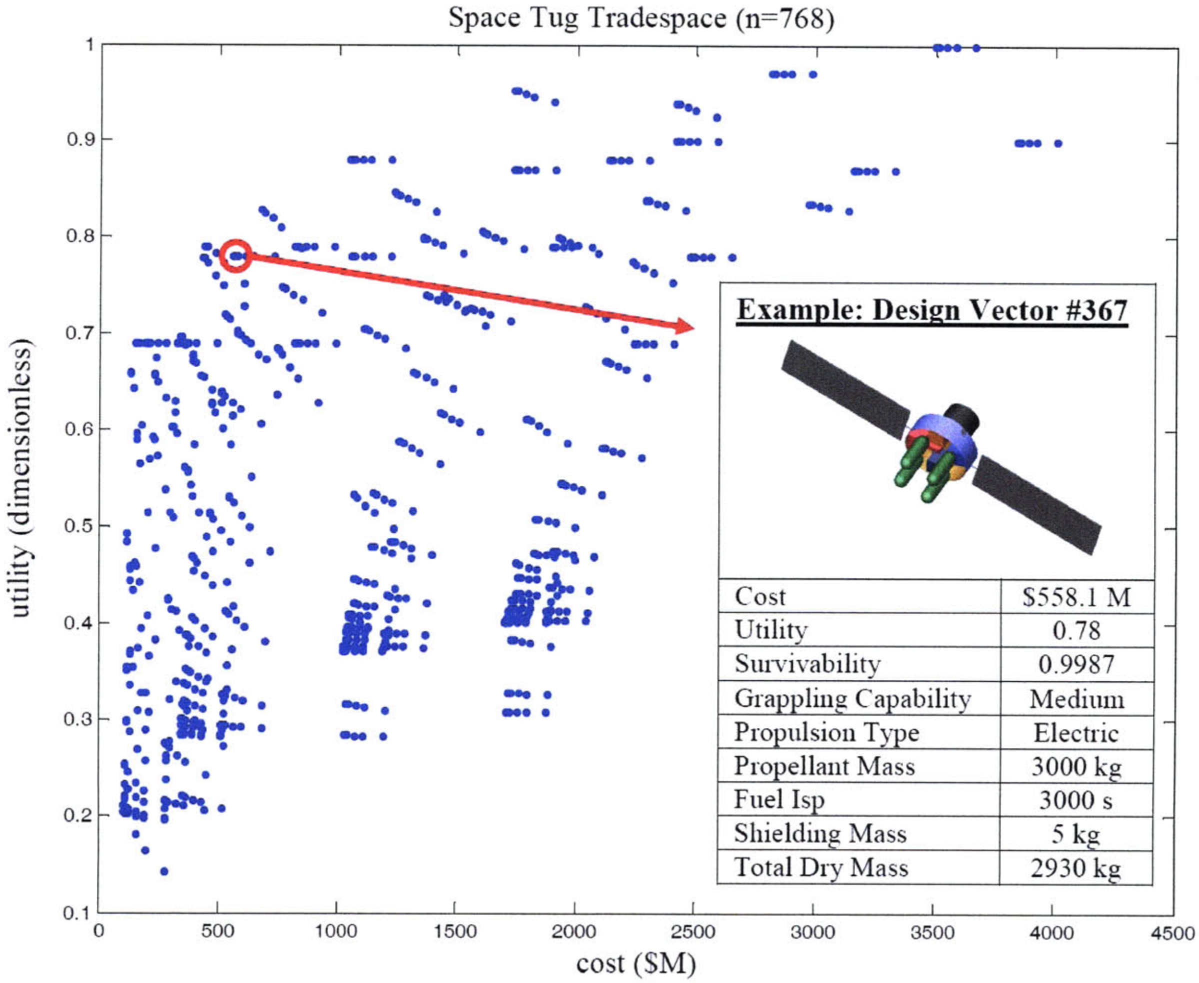
Figure 1-2. Research Focus: System Development Phases 1 and 2 (Ulrich and Eppinger 2004)

1.1.3. Tradespace Exploration

The value-centric perspective is operationalized in conceptual design through the application of decision theory to the engineering design process, making cost-benefit tradeoffs explicit in concept selection (Thurston 1990; Keeney and Raiffa 1993). Extending traditional trade studies, which may consider a small number of alternative designs, tradespace exploration builds on this application by adding computer-based parametric models and simulations, enabling comparison of hundreds or thousands of potential architectures (McManus, Hastings and Warmkessel 2004; Ross et al. 2004). When coupled with decision analysis, tradespace exploration avoids the limits of local point solution trades by providing an understanding of the underlying relationship between the decision-maker preference structure and potential designs. Applied to conceptual design, tradespace exploration may be used as a quantitative tool for evaluating the benefits, costs, and risks of alternative architectures—informing critical front-end decision-making. In addition to evaluating potential technical capabilities, architecture tradespaces may also be used to explore the implications of policy uncertainties (Weigel and Hastings 2004) and changing value perceptions (Ross 2006). Figure 1-3 shows a sample tradespace for a "space tug" orbital transfer vehicle. Each point represents a unique design alternative which was evaluated in terms of lifecycle cost and utility[2] using a parametric computer model.

[1] While the term stakeholder refers to any entity with an interest in the outcome of a system development, the term decision-maker refers to the stakeholder with control over the resources for system development.

[2] Utility may be defined generally as an ordinal metric of stakeholder satisfaction. In this thesis, utility is used to measure the benefit received by decision-makers.



Cost	$558.1 M
Utility	0.78
Survivability	0.9987
Grappling Capability	Medium
Propulsion Type	Electric
Propellant Mass	3000 kg
Fuel Isp	3000 s
Shielding Mass	5 kg
Total Dry Mass	2930 kg

Figure 1-3. Evaluation of Design Alternatives Using Tradespace Exploration

1.1.4. "-ilities"

Given that non-traditional design criteria—such as flexibility and robustness, collectively referred to as "-ilities"—are increasingly regarded as critical system properties for delivering stakeholder value (Rhodes 2004; McManus and Hastings 2006), ongoing systems engineering research is seeking to establish descriptive taxonomies and prescriptive methods for the incorporation of the "-ilities" in system design (Soban and Mavris 2000; de Weck, de Neufville and Chaize 2004; Fricke and Schulz 2005; Rajan et al. 2005; Ross 2006; McManus et al. 2007; Nilchiani and Hastings 2007; Silver and de Weck 2007). The "-ilities" may be defined as temporal system properties that specify the degree to which systems are able to maintain or even improve function in the presence of change. The "-ilities" explicitly recognize that, in addition to meeting requirements in a static context, the performance of system architectures is defined by an ability to deliver value to stakeholders in the presence of changing operational environments, economic markets, and technological developments (Fricke and Schulz 2005). According to Dr. Marvin Sambur, former Assistant Secretary of the Air Force for Acquisitions (Rhodes 2004), a generalized new definition for robustness applied to military acquisitions means developing systems that are:

- capable of *adapting* to changes in mission and requirements
- *expandable/scalable*, and designed to accommodate growth in capability
- able to *reliably* function given changes in threats and environment
- effectively/affordably *sustainable* over their lifecycle
- developed using products designed for use in various *platforms* and systems
- easily *modified* to leverage new technologies

Despite general agreement on their importance, the "-ilities" are neither well-defined nor easily evaluated in isolation.[3] Operationalizing the "-ilities" for value-based design methods, such as tradespace exploration, is challenging and the subject of ongoing research. For example, after building a descriptive theory of the systems property of changeability, Ross (2006) developed a prescriptive dynamic tradespace methodology with the associated metrics of Pareto Trace and Filtered Outdegree. In building upon the existing theory of changeability, this thesis on survivability focuses on the particular challenges posed by dynamic disturbance environments and on how survivability might be better articulated, generated, and evaluated during the conceptual design of engineering systems.

1.2. Motivation

"Our spacecraft, which take 5 to 10 years to build, and then last up to 20 in a static hardware condition, will be configured to solve tomorrow's problems using yesterday's technologies" (Brown 2007).

A typical space system architecture is comprised of one or more satellites, launch vehicle(s) for transportation to operating orbits, ground-based control stations, and communications links among these nodes to transfer information to end users. With the exception of select civil space systems, such as the Hubble Space Telescope and International Space Station, that employ on-orbit servicing, current satellite architectures aim to deliver value over time by developing reliable individual space vehicles that operate in an inaccessible, hostile environment. As a result, attempts to apply flexibility and other "-ilities" to space systems are tightly constrained by the lack of capability to physically service satellites following launch (Richards 2006). A distinguishing characteristic of the current U.S. space architecture is a high level of risk aversion stemming from the high cost of space systems combined with the criticality of space mission areas (on the government side) and drive for investor return (on the commercial side). This environment has driven satellite designers toward three common design strategies: redundancy,[4] proven technology,[5] and long operational lives (Long, Richards and Hastings 2007).

[3] Recognizing that design navigates among functional, physical, and environmental domains (Simon 1996), McManus and Richards et al. (2007) developed the "-ilities Space" to characterize the operational "-ilities" as temporal motion along three axes: needs (*i.e.*, value domain), system (*i.e.*, technical domain), and context (*i.e.*, environmental domain). Section 3.1 provides a detailed description of the "-ilities Space".

[4] Space systems incorporate massive redundancy to mitigate the risk of component failure. Components may fail due to design flaws, emergent interaction effects with other spacecraft systems, exposure to the harsh environment of space, or other random events. Incorporating redundancy leads to very complex systems, increasing spacecraft mass and cost. Furthermore, the value of redundant systems is only realized in the event of component failure.

[5] As a response to the risk-averse nature of the satellite industry, designers are pressured to incorporate proven (*i.e.*, legacy) hardware on space systems. For example, NASA uses Technology Readiness Levels (TRL) as a metric for

1.2.1. Unintended Consequences of Current Satellite Paradigm

The high cost of launching spacecraft combined with a focus on traditional strategic measures of effectiveness in the space industry (*e.g.*, optimize cost-per-function) have driven U.S. space architecture from an era of single-payload, short-lived spacecraft to a current state of multi-payload, long-lived systems. Figure 1-4 depicts the growth in the average design life of active geosynchronous satellites from under two years in 1965 to over thirteen years in 2003 (Sullivan 2005). While this design philosophy is justified on the basis of economic arguments associated with the high initial cost of spacecraft and enabled by improvements in supporting subsystems (*e.g.*, ion propulsion), this design philosophy also has many negative implications. For example, noting that space system developments now take five to ten years, Brown (2007) describes how "complexity has bred fragility" in terms of unanticipated modes of failure. Such unanticipated modes of failure include an acquisitions crisis (Young, Hastings and Schneider 2003) where development problems with an individual sensor can cripple the schedule and budget of multi-payload programs (*e.g.*, the National Polar-Orbiting Environmental Satellite System), software-related common-cause failures that circumvent margin and redundancy (Leveson 2004), and uncertain technological change.[6]

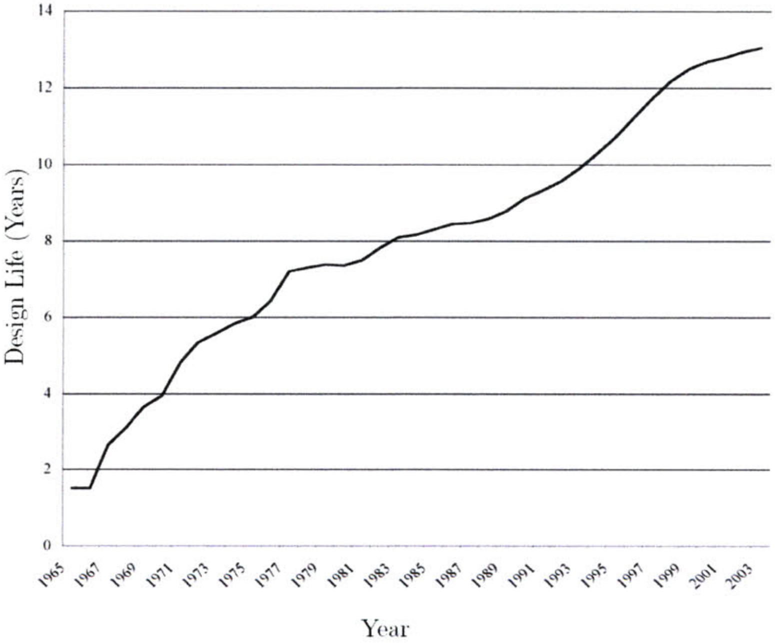


Figure 1-4. Average Design Life of Geosynchronous Satellites (Sullivan 2005)

The consequences of failure for space architecture reliant upon integral, long-lived satellites are further exacerbated by three trends: (1) the growth of military and commercial dependency on

technological maturity. Classified on a scale of one through nine, most spacecraft designs require a TRL of at least eight to insure "flight qualified" hardware. While use of proven technology helps to mitigate mission risk, it also has the negative effect of limiting satellite performance and stalling industry innovation.

[6] One downside of long design lifetimes is the inability to update space-based capabilities with modern avionics in a timely manner during an era dictated by "Moore's Law" (*i.e.*, the doubling of processing speed of new computer chips every 18-24 months). This slowdown of the space industry's "clockspeed" limits the agility of satellite operators in capturing emergent terrestrial markets (Saleh et al. 2006).

space systems (Gonzales 1999; GAO 2002; Ballhaus 2005), (2) the proliferation of threats (Rumsfeld, Andrews et al. 2001; Joseph 2006), and (3) the weakening of the sanctuary view in military space policy (Mowthorpe 2002; O'Hanlon 2004; U.S. 2006; Covault 2007).

1.2.2. Growth of Dependency on Space Systems

An analysis of recent history indicates that military and commercial stakeholders are increasingly dependent on space capabilities. On the military side, space capabilities have extended beyond the strategic missions of the Cold War (*e.g.*, national technical means of treaty verification, missile warning, communications for National Command Authority) to tactical applications (*e.g.*, situational awareness, command and control, navigation). Former Secretary of the U.S. Air Force James Roche states that, "For the first time in our history, space has become an equal partner to air breathers [aircraft] (Ballhaus 2005)." Dr. William Ballhaus, former CEO of the Aerospace Corporation, adds that "Whether in communications, precision weapons, or surveillance—space has changed the way wars are fought." For example, the U.S. used 30 times more satellite bandwidth in Operation Iraqi Freedom for military communications than in Desert Storm (Ballhaus 2005) despite the deployment of fewer troops in the second Persian Gulf War. On the commercial side, space capabilities have also become a major component of the national and global economies, accounting for $85 billion in revenue in 2000 (GAO 2002). Commercial satellite services have become vital to the operation of critical infrastructures, including telecommunications, transportation, electrical power, water supply, gas and oil storage and transportation, emergency services, banking and finance, and continuity of government services; for instance, a 1998 failure of the Galaxy IV satellite disrupted 45 million pagers for three days and blocked credit card authorization at point-of-sale terminals such as gasoline pumps (Joseph 2006).

1.2.3. Proliferation of Threats

Despite the high dependency of government and commercial stakeholders on space capabilities, satellite architectures have become increasingly vulnerable to a growing number of threats. In addition to the challenges posed by severe spacecraft-environment interactions (*e.g.*, growing vulnerability of miniaturized electronics to solar flares) (Hastings and Garrett 1996; Fulghum 2007), designers must also consider the threats posed by malevolent action (Black 2000). As space has become a critical enabler of tactical U.S. military operations, and since the U.S. accounts for approximately 90% of the world's military space expenditures (O'Hanlon 2004), countermeasures against space assets are a developing asymmetric threat (Thomson 1995). For example, China's successful test of an anti-satellite (Asat) weapon against an aging Chinese Feng Yun 1C weather satellite in January 2007 has incited calls for enhancing spacecraft survivability (Covault 2007). The Asat test underscores several of the findings of the 2001 Rumsfeld Commission to Assess U.S. National Security Space Management and Organization: (1) that satellites are vulnerable to a broad spectrum of hostile acts (*e.g.*, denial and deception, interference, jamming, microsatellite attacks, nuclear detonation), (2) that the impact of such surprise attacks could constitute a "Pearl Harbor" in space, and (3) that there is a need to increase spending on space surveillance and control measures (Rumsfeld, Andrews et al. 2001). While the recommendations of the Rumsfeld Space Commission regarding military space policy are subject to debate (O'Hanlon 2004), it is important to note the severity of the potential impact of an attack on U.S. space assets (CRS 2004) and that such vulnerabilities extend to unsecured commercial systems upon which government users are dependent (GAO 2002).

1.2.4. Weakening Sanctuary School in Military Space Policy

The importance of addressing the fragility of current space architectures is underscored by the weakening of the sanctuary view of space in U.S. military space policy. Mowthorpe (2002) outlines four schools of thought in military space power theory: (1) the *sanctuary view* that believes space should not be used as a platform for basing weapons, (2) the *survivability view* that believes space forces are inherently less survivable and should not be depended upon for wartime functions, (3) the *space control view* which applies the concepts of air superiority and sea control to space, and (4) the *high ground view* that believes force application from space will become a critical determinant of military power. With a focus on utilizing satellites for reconnaissance purposes, the sanctuary school dominated military space policy in the Cold War through the 1970's. While the Reagan and first Bush administrations laid the foundation for a future policy of space control through research and development activities (*e.g.*, 1985 test of an Asat against a satellite, Strategic Defense Initiative) (Mowthorpe 2002), the Clinton administration scaled back space control programs before they became operational (*e.g.*, shifting missile defense efforts back from strategic to theater systems). However, technology development for space control continued (O'Hanlon 2004). During this decade, the actions and policy statements of the current Bush administration reflect the completion of a shift from the sanctuary view to the space control view. For example, the 2002 withdrawal of the United States from the 1972 Anti-Ballistic Missile Treaty now enables the possibility of space-based missile defense. Furthermore, the release of a new National Space Policy (2006) that compares the importance of "freedom of action in space" with air power and sea power directly aligns with space control doctrine.

1.2.5. Synthesis

Given that the need to address space architecture fragility has been articulated by national leaders, a critical challenge arises: how best to enhance the survivability of space architecture? Are existing survivability practices of hardening individual satellites or constellations applicable to these problems? Are there alternative architectures that are intrinsically survivable? For example, to what extent might architectural agility be emphasized to address the mismatch between rapidly changing environments and the 15-25 year generational turnover of satellites (GAO 2006)? Furthermore, given a set of candidate designs, how might alternatives be systematically evaluated—gaining knowledge regarding the stakeholder value proposition, mission context, technical performance of candidate designs—in order to down-select to a small number of alternatives before entering the more costly detailed design and production phases of system development.

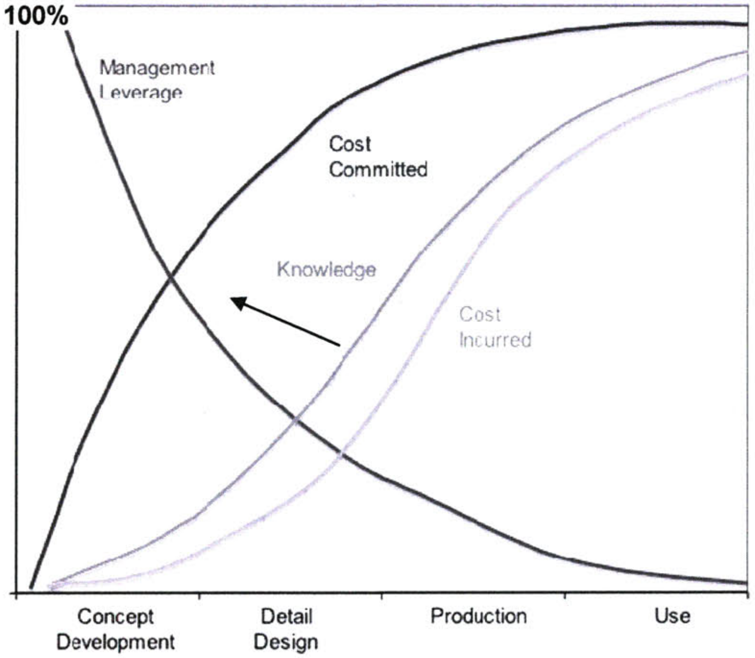


Figure 1-5. Goal of Front-End Analysis in Complex System Development

Figure 1-5 illustrates the motivation for and general challenge of system analysis: generation and evaluation of alternatives to increase decision-maker knowledge while management leverage is high and committed costs are low.

1.3. Scope

1.3.1. Relevant Literature

Technology, management, and policy literatures are consulted to inform all research phases and to position the unique contributions of the dissertation relative to previous work (Figure 1-6). Specific disciplinary areas include engineering systems (*e.g.*, uncertainty management), systems engineering and architecting (*e.g.*, decision analysis, system architecture, tradespace exploration), survivability engineering (*e.g.*, combat aircraft design), space policy, and defense acquisitions. The literature review will particularly focus on understanding the strengths and weaknesses of existing theories and methods of survivability engineering.

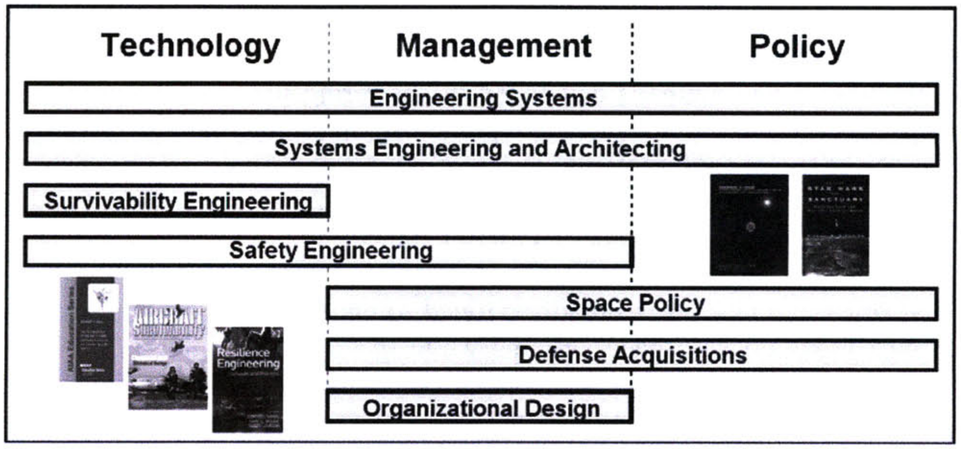


Figure 1-6. Relevant Literature

1.3.2. Research Questions

The following research questions are posed to address the survivability challenges identified in Section 1.2 while leveraging the emerging dynamic tradespace exploration methods discussed in Section 1.1.[7] The overarching goal is to develop and test a new system analysis methodology for survivability that empowers designers to evaluate dynamically relevant systems in hostile environments.[8]

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

The first research question aims to conceptualize and operationalize survivability for subsequent investigation. A general definition of survivability is a critical first step because existing metrics for survivability vary among domains and are traditionally calculated with specific operational scenarios in mind. The goal of the second question is to develop a framework of structural and behavioral principles that enable survivability across the entire lifecycle of disturbances. The principles are to provide designers with a portfolio of concept-neutral strategies for achieving survivability during concept generation. Existing sets of survivability design principles tend to exclude non-physical factors and to focus on concept-specific techniques. The third question identifies the core challenge of the proposed research: quantification of a particular "-ility" to enable its specification, evaluation, and verification during the conceptual design of aerospace

[7] Chapter 2, Problem Formulation, provides a more detailed rationale for the four research questions.

[8] Implicit in the research questions are two hypotheses: (1) that survivability can be articulated in the design process as a dynamic, value-centric system property and (2) that dynamic tradespace analysis can be used to assess system survivability in hostile environments.

systems. Despite the general agreement regarding the importance of the "-ilities", they are neither well-defined nor easily evaluated in isolation. Finally, the purpose of the fourth question is to apply the theories and methods developed in answering the previous questions to current design issues in space system architecture. In particular, emerging military space radar concepts will evaluated across threat environments. Addressing this question is of vital importance to the U.S., given the tens of billions of dollars at stake and the cyclical establishment and cancellation of space radar programs over the past decade (CBO 2007).

While the first research question is broadly defined to encompass all engineering systems, the second and third focus on aerospace systems while the fourth specializes on space systems. There are three reasons for narrowing the scope of successive research questions: (1) to leverage the researcher's academic background and professional experience, (2) to accommodate finite time and resources, and (3) to maximize the impact of the research on government and industry. While the research questions provide for testing the survivability design methodology in the domain of aerospace systems, the methodology will be constructed for broad applicability. Therefore, an output of the research is a hypothesis for future work: that the survivability theories and methods apply to all engineering systems.

1.3.3. Contributions

The fundamental contribution of the research is a clarification of how uncertain future environments impact current and future system design options. In proposing an integrated methodology for the specification, evaluation, and verification of survivability in conceptual design, the general challenge of incorporating a larger set of "-ilities" in systems engineering will be addressed. Specific contributions include:

- Framework for precisely defining survivability and specifying relationships to "-ilities"
- Dynamic, value-centric conceptualization of survivability
- Portfolio of design principles for survivability
- Extensions of dynamic tradespace exploration to incorporate environmental perturbations
- Evaluation of performance, cost, and survivability of alternative future military space radar concepts

Four ongoing ESD research challenges are addressed in the research: uncertainty management, application of interdisciplinary methods, enterprise issues, and stakeholder complexity. In establishing a descriptive taxonomy and prescriptive methodology for the incorporation of the "-ilities" in system design, the research integrates methods from disciplines across engineering and the natural and social sciences. For example, Multi-Attribute Tradespace Exploration (MATE) combines engineering design with economics, optimization, physics, psychology, and decision theory. Interactions with government system program offices and system analysts in industry to gather lead user feedback and apply the tradespace exploration methodology to ongoing system developments have ensured that enterprise implementation issues are addressed. Finally, competing stakeholder priorities are a key motivator for a survivability tradespace methodology as stakeholders frequently possess very different perspectives on trade-offs between mission performance and survivability.

1.4. Approach

To address the four research questions, a four-step research methodology is followed: (1) knowledge capture and synthesis, (2) theory development, (3) computer experimentation, and (4) case applications (Ross 2006). Figure 1-7 depicts the relationships among these four general phases of the research process. Each phase is not a discrete step in a serial process but rather one aspect of an iterative, concurrent process of continuous learning, revisiting of assumptions, and development and testing of theory. Both qualitative and quantitative methods are employed.

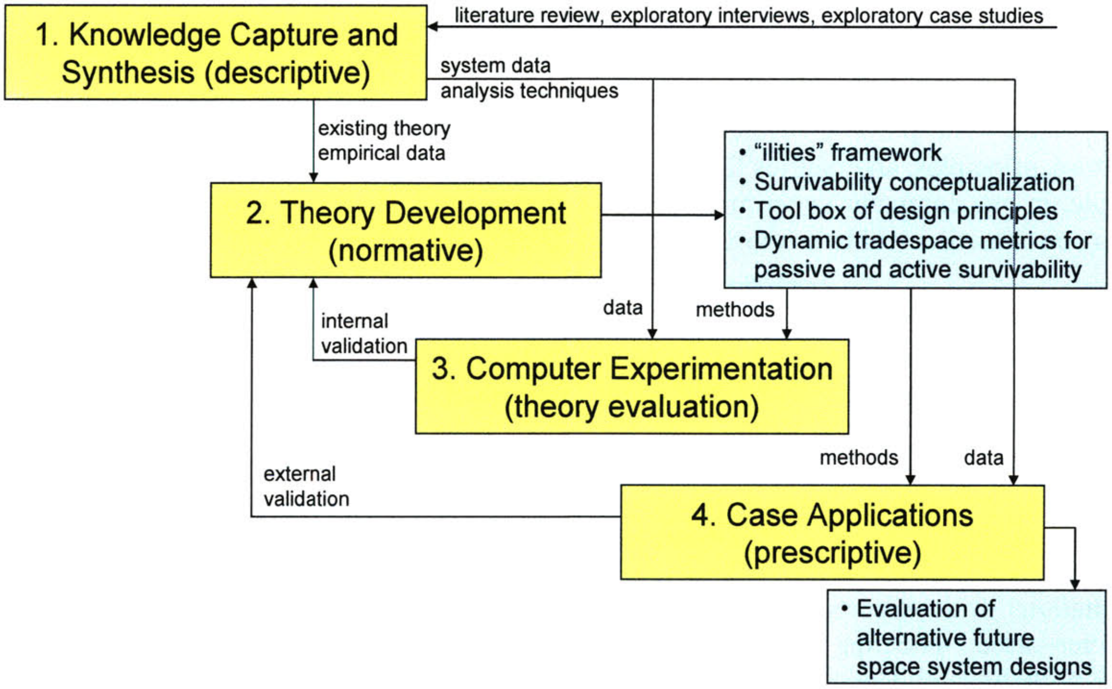

1. Knowledge Capture and Synthesis (descriptive)
literature review, exploratory interviews, exploratory case studies
system data
analysis techniques
existing theory
empirical data
2. Theory Development (normative)
• "ilities" framework
• Survivability conceptualization
• Tool box of design principles
• Dynamic tradespace metrics for passive and active survivability
data
methods
internal validation
3. Computer Experimentation (theory evaluation)
methods
data
external validation
4. Case Applications (prescriptive)
• Evaluation of alternative future space system designs

Figure 1-7. Research Design

1.4.1. Knowledge Capture and Synthesis

The first phase, knowledge capture and synthesis, is descriptive and focuses on providing a detailed picture of how survivability is articulated in conceptual design, categorizing existing definitions and methods, and gathering technical data on engineering systems. Data in the descriptive phase is gathered from a broad set of technology, management, and policy literatures (*e.g.*, engineering systems, systems engineering and architecting, survivability engineering, space policy, defense acquisitions); exploratory interviews with key stakeholders and senior system architects (to motivate and inform the research, not for statistical significance); and technical specifications of existing aerospace systems deemed survivable. The primary outputs of the knowledge capture and synthesis phase are a general conceptualization of survivability that leverages previous theory and empirical data to ground the subsequent theoretical investigation. This phase provides methodological insights and system data to the computer experimentation and case application phases.

1.4.2. Theory Development

The second phase, theory development, focuses on exploring the distinguishing characteristics of survivability and the "-ilities", understanding the design principles that achieve survivability for aerospace systems, and determining how to quantify survivability as a decision metric for dynamic tradespace exploration. Informed by the existing theories and empirical data synthesized in the previous phase, this normative survivability design methodology is deployed and tested in the computer experimentation and case applications phases of the research.

1.4.3. Computer Experiments

In the third phase, computer experiments are used to map the descriptive research conducted during knowledge capture and synthesis to the normative work performed during theory development. The purpose of the computer experiments is to test the proposed survivability definition, principles, and metrics for internal validity in a controlled modeling environment. For example, in one computer experiment, satellite survivability against orbital debris is added as a design consideration within an existing orbital transfer vehicle tradespace.

1.4.4. Case Applications

In the fourth phase, case applications are conducted to test the prescriptive value of the new survivability theory in the "messy" real world. As a qualitative check for the external validity of the survivability design principles, the survivability features of existing, highly-survivable aerospace systems are inductively mapped to the proposed set of principles. As a quantitative check for the external validity of the survivability metrics, the theoretical insights from phase two are deployed in dynamic tradespace exploration study of military space radar. This case application includes interviews with system stakeholders to elicit multi-attribute utility functions; consultations with experts to gather sets of potential hostile operating environments; and computer-based modeling and simulation to assess differential cost, performance, and survivability of candidate space system architectures.

A key aspect of testing the external validity of the proposed methodology is to apply the research to ongoing system developments with critical survivability requirements. To meet this goal, lead user feedback has been gathered from government system program offices and practitioners in industry and incorporated into the dissertation.

1.5. Structure of Thesis

Eight chapters follow this introduction. Figure 1-8 provides an overview of the thesis structure.

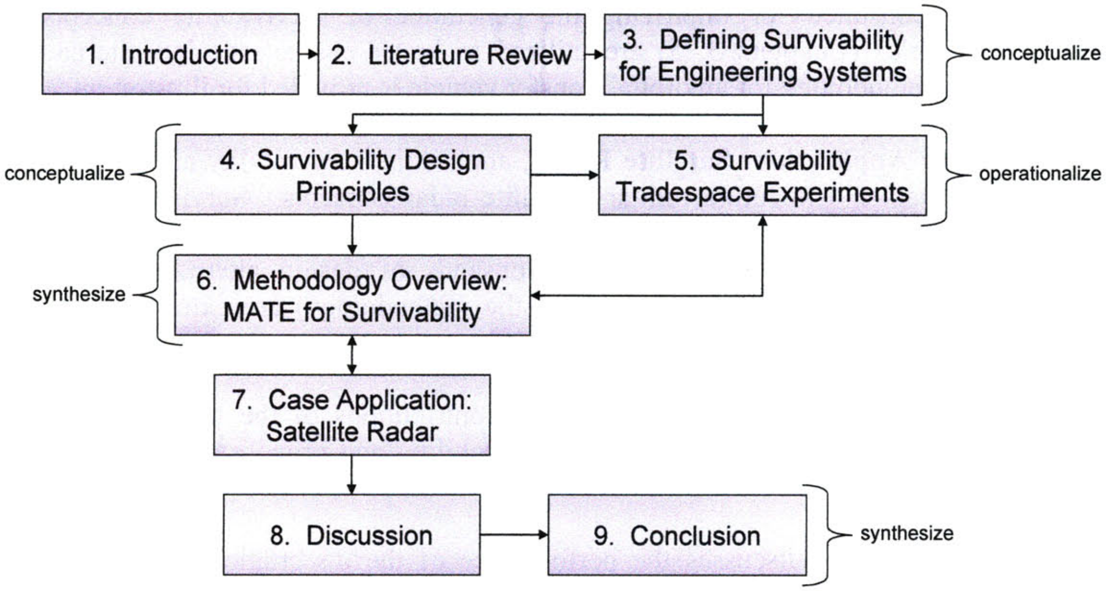

1. Introduction
2. Literature Review
3. Defining Survivability for Engineering Systems
conceptualize
conceptualize
4. Survivability Design Principles
5. Survivability Tradespace Experiments
operationalize
synthesize
6. Methodology Overview: MATE for Survivability
7. Case Application: Satellite Radar
8. Discussion
9. Conclusion
synthesize

Figure 1-8. Structure of Thesis

Chapter 2, Problem Formulation, surveys existing methods associated with design for survivability to identify knowledge gaps and to inform the subject and scope of the problem statement. The dissertation's guiding research questions (introduced in Section 1.3.2) stem directly from this problem statement.

Chapter 3, Defining Survivability for Engineering Systems, answers the first research question by presenting a general conceptualization of survivability. In addition, an "-ilities" framework is described that relates survivability to other "-ilities", such as flexibility and robustness.

Chapter 4, Survivability Design Principles, addresses the second research question by presenting a set of seventeen principles spanning Types I, II, and III survivability. The principles are derived using deductive and inductive means. The principles are applied to existing, survivable, aerospace systems—including the A-10 Thunderbolt II combat aircraft, UH-60A Blackhawk helicopter, Iridium satellite communications system, and F-16C "Fighting Falcon" combat aircraft—as empirical tests of external validity.

Chapter 5, Survivability Tradespace Experiments, answers the third research question by operationalizing the conceptual definition of survivability (introduced in Chapter 3) in experimental tradespaces for an orbital transfer vehicle. Two new survivability metrics, *time-weighted average utility loss* and *threshold availability*, are presented and shown to be discriminating metrics for navigating survivability tradespaces of thousands of design alternatives.

Chapter 6, Methodology Overview: MATE for Survivability, answers the fourth research question by synthesizing lessons learned in the preceding chapters. In addition to leveraging existing modeling techniques found in the literature (Chapter 2), the design principles framework (Chapter 4) is consulted for improving the generation of survivability concepts and the survivability metrics (Chapters 3, 5) are utilized to better evaluate design alternatives. An example of the methodology for an orbital transfer vehicle is provided for illustration.

Chapter 7, Case Application: Satellite Radar, applies the survivability analysis methodology introduced in Chapter 6 to future military satellite radar concepts. Survivability "tear(drop)" tradespaces and response surfaces are used to conduct integrated trades among lifecycle cost, multi-attribute utility, and survivability of thousands of design alternatives. Prescriptive technical insights (for both satellite radar and the methodology) are extracted from the case application.

Chapter 8, Discussion, synthesizes the unique contributions of the thesis, analyzes several implementation issues regarding MATE for Survivability, and proposes several areas of future work.

Chapter 9, Conclusion, discusses the performance of the dissertation across the objectives identified in the introduction and draws general conclusions.

A spiral development approach was pursued for the development and maturation of the theories and methods proposed in this dissertation. From the initiation of the research in September 2006, several conference papers were completed and presented to gather feedback on preliminary concepts and ideas. Table 1-1 lists the papers from which much of the content of this dissertation is derived. The author is grateful for the opportunity to collaborate on his research with faculty, staff, and students associated with MIT's Systems Engineering Advancement Research Initiative (SEAri).

Table 1-1. Mapping of Completed Papers to Thesis Chapters

Conference Paper	Chapter(s)
Richards, M., Hastings, D., Rhodes, D., and Weigel, A., "Systems Architecting for Survivability: Limitations of Existing Methods for Aerospace Systems," *6th Conference on Systems Engineering Research*, Los Angeles, CA, April 2008.	1, 2
Richards, M., Hastings, D., Rhodes, D., and Weigel, A., "Defining Survivability for Engineering Systems," *5th Conference on Systems Engineering Research*, Hoboken, NJ, March 2007.	1, 3, 4
McManus, H., Richards, M., Ross, A., and Hastings, D., "A Framework for Incorporating "ilities" in Tradespace Studies," *AIAA Space 2007*, Long Beach, CA, September 2007.	3, 5
Richards, M., Ross, A., Shah, N., and Hastings, D., "Metrics for Evaluating Survivability in Dynamic Multi-Attribute Tradespace Exploration," *AIAA Space 2008*, San Diego, CA, September 2008.	3, 5, 8
Richards, M., Ross, A., Hastings, D., and Rhodes, D., "Design Principles for Survivable System Architecture," *1st IEEE Systems Conference*, Honolulu, HI, April 2007.	4
Richards, M., Ross, A., Hastings, D., and Rhodes, D., "Two Empirical Tests of Design Principles for Survivable System Architecture," *18th INCOSE Symposium*, Utrecht, Netherlands, June 2008.	4
Richards, M., Ross, A., Hastings, D., and Rhodes, D., "Empirical Validation of Design Principles for Survivable System Architecture," *2nd IEEE Systems Conference*, Montreal, Canada, April 2008.	4
Richards, M., Ross, A., Hastings, D., and Rhodes, D., "Multi-Attribute Tradespace Exploration for Survivability," *7th Conference on Systems Engineering Research*, Loughborough, England, April 2009.	6
Richards, M., Ross, A., Hastings, D., and Rhodes, D., "Survivability Design Principles for Enhanced Concept Generation and Evaluation," *19th INCOSE Symposium*, Suntec City, Singapore, July 2009.	6, 7
Ross, A., McManus, H., Long, A., Richards, M., Rhodes, D., and Hastings, D., "Responsive Systems Comparison Method: Case Study in Assessing Future Designs in the Presence of Change," *AIAA Space 2008*, San Diego, CA, September 2008.	7
Roberts, C., Richards, M., Ross, A., Rhodes, D., and Hastings, D., "Scenario Planning in Dynamic Multi-Attribute Tradespace Exploration," *3rd IEEE Systems Conference*, Vancouver, Canada, March 2009.	7
Richards, M., Ross, A., Stein, D., and Hastings, D., "Multi-Attribute Tradespace Exploration for Survivability: Application to Satellite Radar," *AIAA Space 2009*, Pasadena, CA, September 2009.	7
Richards, M., Viscito, L., Ross, A., and Hastings, D., "Distinguishing Attributes for the Operationally Responsive Space Paradigm," *6th Responsive Space Conference*, Los Angeles, CA, April 2008.	8
Shah, N., Richards, M., Broniatowski, D., Laracy, J., Springmann, P., and Hastings, D., "System of Systems Architecture: The Case of Space Situational Awareness," *AIAA Space 2007*, Long Beach, CA, September 2007.	8

2. Problem Formulation

This chapter formulates the challenge of designing for survivability as a problem requiring an enhanced tradespace exploration methodology within the context of current survivability engineering and system analysis methodologies. After reviewing current state-of-the-art survivability engineering and system analysis methodologies (Sections 2.1 and 2.2, respectively), the limitations of the current approaches to survivability engineering during conceptual design are discussed (Section 2.3). The chapter concludes with a formal problem statement (Section 2.4).

2.1. State-of-the-Practice: Survivability Engineering

Survivability is defined by system engineers as "the capability of a system to avoid or withstand hostile natural and manmade environments without suffering abortive impairment of its ability to accomplish its designated mission" (USAF 2005). According to the Department of Defense (DoD) Regulation 5000.2-R, survivability consists of susceptibility, vulnerability, and recoverability (DoD 2002):

> ***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).
>
> ***Susceptibility***. The degree to which a weapon system is open to effective attack due to one or more inherent weakness (AP3.2.7).
>
> ***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).

Although primarily 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 hazards (GAO 2002). While disturbances may originate from a wide range of hostile natural and synthetic environments, a universal challenge confronting system engineers is the specification, development, procurement, operation, and maintenance of systems with critical survivability requirements (Neumann 2000).

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).

Rather than attempting to broadly survey all application areas of survivability engineering, Section 2.1 focuses on summarizing the state-of-the-practice of survivability characterization, quantification, and analysis in aerospace system design. Following a brief note on the historical evolution of the survivability discipline, the acquisition process, analytic frameworks, and evaluation techniques underlying modern survivability engineering are discussed. The section concludes with a mapping of survivability engineering to related disciplines such as system safety and security engineering.

2.1.1. Historical Context

While the practice of survivability engineering extends back as long as humans have utilized synthetic artifacts in hostile environments, the modern discipline emerged from the First and Second World Wars. After being developed within the context of naval ship design and applied to combat aircraft soon thereafter, the discipline's ascendancy has paralleled the rise of the modern system sciences—particularly systems engineering, systems analysis, and operations research (Johnson 1997).

Survivability research stems from a long history of naval architecture that sought to prevent the loss of ships from sustained damage and to save lives in the event of a ship sinking (Yurick and Doss 2002). Modern research on survivability engineering is an outgrowth of experience in the First and Second World Wars and became a formal discipline in the domain of combat aircraft. Ball and Atkinson (1995) document the history of combat aircraft survivability engineering from the 1940's to the present day. While the importance of survivability was recognized during the Second World War (*e.g.*, eight major design evolutions made to the B-17 "Flying Fortress" between 1942 and 1945 to enhance survivability), survivability was not specified as a formal design requirement by the military for another 25 years. Before the systems approach for survivability engineering existed, enhancements were made within the context of individual aircraft design disciplines and subsystems (*e.g.*, structures made more resistant to enemy fire, guns and missiles added for self-defense) and relied on combat experience to adapt designs to more survivable states. Following the loss of 5,000 aircraft by the U.S. military in Southeast Asia between 1963 and 1973, the importance of the survivability of military aircraft increased dramatically, and a formal discipline emerged to support the integrated specification, design, and assessment of highly survivable systems (Ball and Atkinson 1995).

2.1.2. Survivability in U.S. Military Acquisitions

U.S. military acquisition policy requires that survivability be systematically incorporated into current and future weapons systems. While the Army, Navy, and Air Force each have specific policies for implementing an integrated survivability program plan in major acquisition programs, all of the departments base their programs on DoD Regulation 5000.2-R (Ball 2003). According the Section C5.2.3.5.12 of DoD Regulation 5000.2-R,[9] systems "shall be survivable to the threat levels anticipated in their projected operating environment…without the crew suffering acute chronic illness, disability, or death." In particular, program managers are instructed to establish and maintain a survivability program throughout the system lifecycle, including a full assessment of system survivability against "all anticipated threats at all levels of conflict, early in

[9] See page 95 of DoD Regulation 5000.2-R: *Mandatory Procedures for Major Defense Acquisitions Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs,* (Program Design, Systems Engineering Survivability), at http://exploration.nasa.gov/documents/TTT_052005/DoD50002R.pdf.

the program, but in no case later than entering system demonstration or equivalent." DoD Regulation 5000.2-R also stresses the importance of considering mission effectiveness by seeking to maximize survivability enhancement features—including threat avoidance, hardening, and rapid reparability—while minimizing the impact on overall program cost and schedule (DoD 2002).

The survivability program plan is implemented within the context of the defense acquisition management framework (Figure 2-1). DoD Instruction 5000.2, *Operation of the Defense Acquisition System*, describes the DoD's event-oriented process of translating mission needs into weapon systems (DoD 2003b). In general, each procurement effort is divided into four discrete phases: (1) concept refinement, (2) concept and technology development, (3) system development and demonstration, and (4) production, deployment, and sustainment. The four phases are separated by key decision points called milestones. During concept refinement, key performance parameters are specified based on user needs and a preliminary concept-of-operations (CONOPS) is established. During concept and technology development, technical feasibility and desirability of the system is further examined before a decision is made as to whether to make the system a formal acquisition program (Milestone B). During system development and demonstration, the detailed design of the system is completed, culminating in a critical design review (Milestone C). Following success at Milestone C, authorization is given to proceed to fabrication, testing, and deployment of the system during the fourth and final phase.

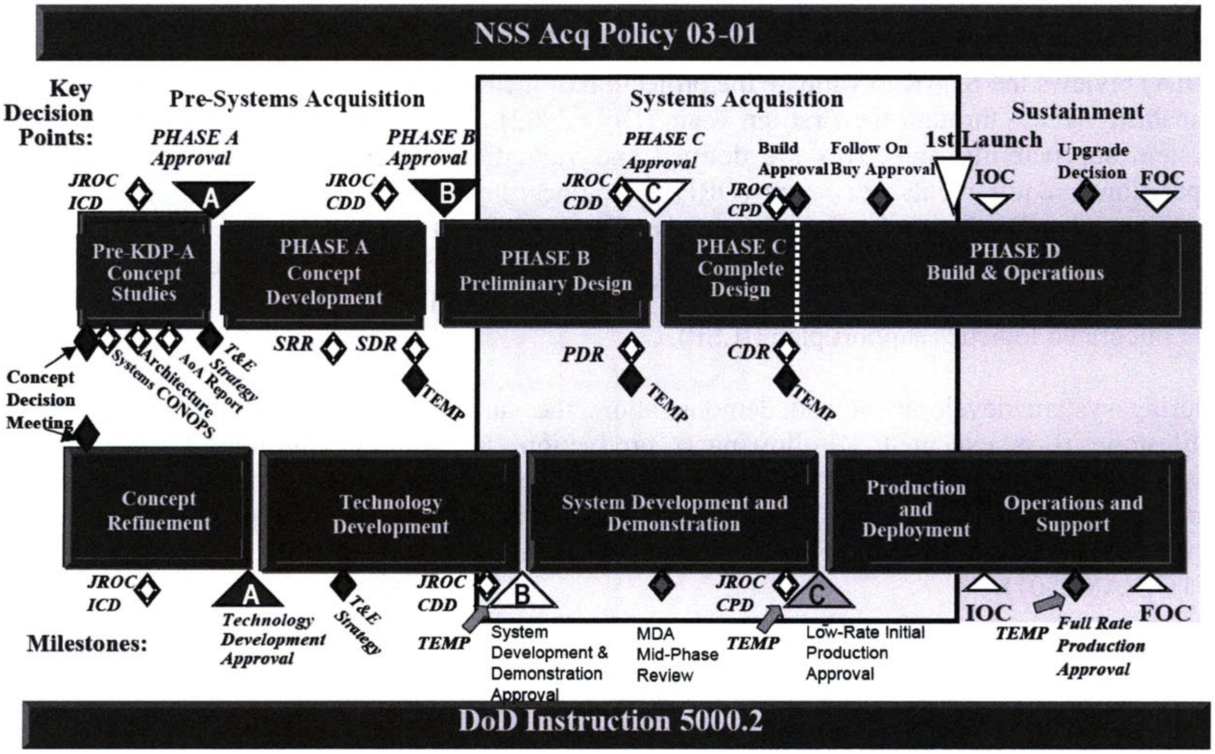


Figure 2-1. Defense Acquisition Management Framework (USAF 2005)

Given the diversity of programs procured by the DoD, Instruction 5000.2 recognizes that every program is unique and may not need to follow the entire process. For example, decision-making for national security space (NSS) acquisitions is focused on the earlier phases of the lifecycle given the emphasis on "high-tech," small-quantity programs. This is in contrast to the DoD 5000 model that is focused on making the best large quantity production decision (*e.g.*, conducting low-rate initial production and testing of Joint Strike Fighter before committing to thousands of production units). These differences are reflected in NSS Acquisition Policy 03-01 (DoD 2004) which phases milestones earlier than the DoD 5000 model (as observed in Figure 2-1) and customizes acquisition activities for satellite development.

Survivability engineering activities occur across all four phases of the system lifecycle (Ball 2003). During concept refinement, expected operational environments are discussed in the mission needs statement (MNS). These operational environments may include conventional, electronic, nuclear, biological, chemical, terrorist, and sabotage threats.

During concept and technology development, operational threats are formally specified, survivability objectives are established, and survivability considerations are incorporated into test and sustainment plans (Ball 2003). The foundation of the survivability program plan is the system threat assessment report (STAR). The STAR is issued by a service intelligence agency as an estimate of the operational, physical, and technological environment in which the system is expected to function. The STAR is the authoritative document from which survivability requirements are derived—specifying threat force levels as well as enemy doctrine, strategy, and tactics (Ball 2003). Prior to all milestone decision points, the Defense Intelligence Agency (DIA) reviews the STAR to validate the projection of the threat environment at initial operational capability (IOC) through the first ten years (DoD 2002). Having formally specified the threat, system survivability objectives are defined and validation criteria are established within the operational requirements document (ORD). Engineering models at the engagement, mission, and campaign-levels are developed to analyze the mission effectiveness of design alternatives. Critical survivability issues requiring testing are incorporated into the test and evaluation master plan (TEMP). Facilities required to support unique survivability characteristics are identified in the integrated logistics support plan (ILSP).

During system development and demonstration, the survivability program plan agreed to at Milestone B is executed. Following a production decision at Milestone C, a complete assessment of how well the survivability objectives are addressed is made during the production and deployment phase. If applicable, survivability considerations are incorporated into planned upgrade packages, including plans for retrofitting survivability features into existing systems (JTCG/AS 2001).

In the preceding description of survivability in U.S. military acquisitions, the survivability program plan is neatly decomposed into each phase of the development process. While this elegant decomposition may be preserved in terms of program phase (in the unlikely absence of changing requirements, threats, and technologies), such decomposition is not possible regarding the composition of the functional team focused on survivability. Successful implementation of a survivability program plan requires a system-level approach to integrate subsystem development efforts at the highest levels of program management. The following excerpt from the handbook issued by the Joint Technical Coordinating Group on Aircraft Survivability underscores the need for an interdisciplinary, systems approach.

> The diverse activities and functions associated with the survivability discipline range from analyses of the inherent capability of enemy threats to the effectiveness of those threats in particular environments; from the engineering of survivability design features or enhancements to susceptibility of the system; from test and evaluation and analysis of inherent aircraft vulnerability to damage response of materials to threat impact; from development of analytical assessment procedures to analysis of combat data; and from the development of vulnerability/susceptibility reduction techniques to aircraft trade studies that include and interface with other functional disciplines (maintainability, reliability, *etc.*). This diversity makes the survivability functional discipline multidimensional and interdependent. Close technical working relationships, with interchanges of data and methodology among these activities and functions, require a precise understanding of the processes and terminology used and the full support of program management, systems engineering, and Integrated Product Teams (JTCG/AS 2001).

Having discussed how survivability is implemented within the DoD acquisitions structure, the following section describes the analytic approaches taken by survivability engineers during conceptual design.

2.1.3. Existing Analytic Frameworks

As discussed in the introduction to Section 2.1, variety of domain- and system-specific methodologies exist to assess survivability during front-end design activities. At a fundamental level, most methodologies evaluate survivability enhancement features in terms of minimizing total system lifecycle cost while others seek to optimize the defensive system's cost-exchange ratios with the attacker.

In *The Fundamentals of Aircraft Combat Survivability Analysis and Design*, Ball (2003) provides an excellent overview of the principles and methods of the survivability engineering discipline. According to Ball, design for survivability involves two elements (1) increasing the ability of systems to avoid disturbances (*i.e.*, reduce susceptibility) and (2) increasing the ability of systems to withstand disturbances (*i.e.*, reduce vulnerability). Figure 2-2 outlines Ball's general survivability assessment methodology for combat aircraft.

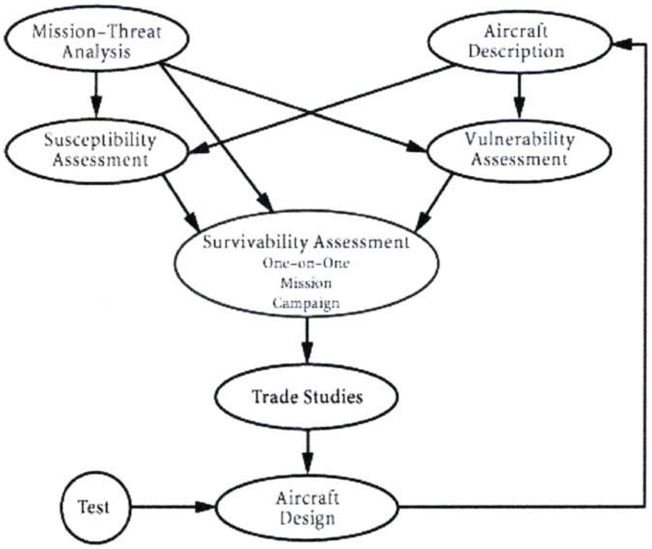
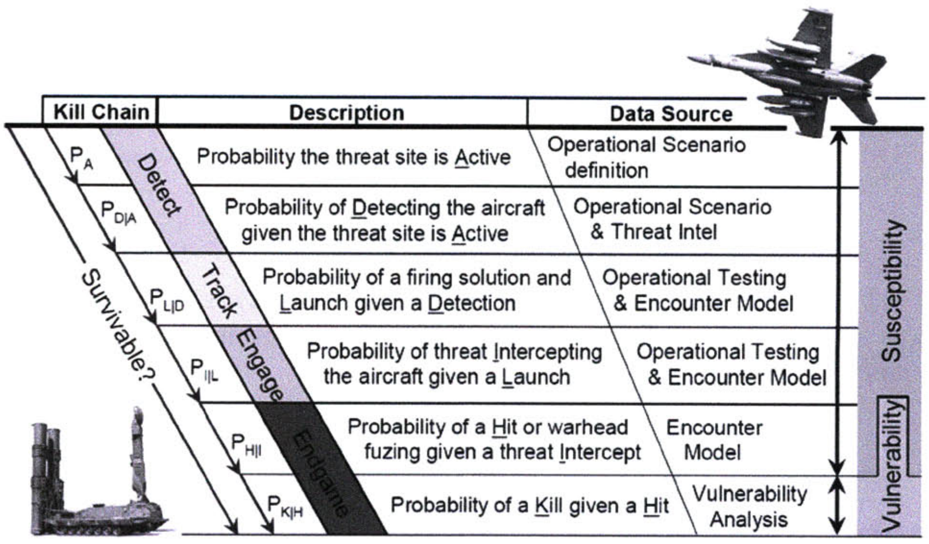


Figure 2-2. Ball's Survivability Assessment Methodology

Because survivability emerges from the interaction of a system with its environment, the survivability methodology is initiated with a mission threat assessment. Having specified the type, strength, command structure, equipment, and disposition of the enemy force, a detailed model of the aircraft is obtained. Next, the susceptibility and vulnerability assessments are conducted. In a typical susceptibility assessment for a combat aircraft, computer simulations of the anticipated air defense system and live-fire tests are conducted to determine both the likelihood that the aircraft is hit as well as the spatial distribution of hits. In a typical vulnerability assessment, critical aircraft components and their kill modes are identified using fault tree analysis (FTA) and failure mode and effects analysis (FMEA). After making simplifying assumptions (*e.g.*, perpendicular attack direction, uniform distribution of hits over exposed cross-sectional area), computer programs are used to estimate likelihood that the aircraft is killed given a random hit.

Following issuance of the STAR and completion of the susceptibility and vulnerability assessments, survivability assessments of design alternatives are performed for particular engagement, mission, and campaign scenarios. Given that a system's survival in combat is not a deterministic outcome that can be predicted with certainty, survivability is measured by a probability (Ball 2003). For example, at the engagement level, the probability of an aircraft surviving a one-on-one engagement from a single shot from a single weapon is calculated using an event tree (*e.g.*, Figure 2-3). Five probability assignments are used from the susceptibility assessment—P[weapon is active], P[sensor detects], P[fire control solution is obtained], P[weapon intercepts], P[weapon hits]—and one probability assignment is used from the vulnerability assessment—P[weapon hit disrupts critical components]. The probability of surviving the engagement is computed as the complement of the joint probability of these six assigned values. This same process is applied at the mission and campaign level by allowing multiple shots from multiple weapons. In order to abstract away the complexity associated with dependent shot outcome probabilities (*e.g.*, increased aircraft susceptibility and vulnerability if one of an aircraft's four engines is destroyed by a previous engagement), independent shot outcomes are assumed.



Kill Chain	Description	Data Source
P_A	Probability the threat site is Active	Operational Scenario definition
$P_{D\|A}$	Probability of Detecting the aircraft given the threat site is Active	Operational Scenario & Threat Intel
$P_{L\|D}$	Probability of a firing solution and Launch given a Detection	Operational Testing & Encounter Model
$P_{I\|L}$	Probability of threat Intercepting the aircraft given a Launch	Operational Testing & Encounter Model
$P_{H\|I}$	Probability of a Hit or warhead fuzing given a threat Intercept	Encounter Model
$P_{K\|H}$	Probability of a Kill given a Hit	Vulnerability Analysis

Figure 2-3. Kill Chain for Engagement-Level Survivability Assessment (Anderson and Williamsen 2007)

The next step in Ball's survivability assessment methodology is to conduct trade studies to determine the survivability improvements and cost and performance burdens associated with each survivability feature under consideration. The mission and campaign survival rates are computed for both the baseline design and designs incorporating survivability enhancement features. Several other measures-of-effectiveness (*e.g.*, reliability, maintainability, safety, and reparability) are also computed for the designs under consideration. Finally, a campaign measure of effectiveness—typically net lifecycle cost—is selected as the optimization criteria for determining whether to incorporate different combinations of survivability features.[10] Throndson (1982) presents a representative example of this methodological approach, evaluating the impact of various signature reduction and hardening features on a baseline combat aircraft propulsion system.

The final step in Ball's survivability assessment methodology is to test the efficacy of the proposed survivability enhancement features and identify any emergent survivability issues. While survivability testing during conceptual design might involve subscale models, final susceptibility and vulnerability testing usually involves full-scale models for signature measurement and live-fire testing.

The reliance of Ball's methodology on probabilistic risk assessment (Bedford and Cooke 2001) and focus on lifecycle cost minimization is shared by the threat evaluation methodology for satellites documented in the U.S. Air Force Space and Missile Systems Center's *Systems Engineering Primer and Handbook* (USAF 2005). The survivability analysis methodology in the handbook consists of six steps. First, three factors associated with the top-level threats

[10] Depending on the number of survivability enhancement features and levels under consideration, the number of operational scenarios under investigation, and the availability of computing resources for modeling and simulation, it may be burdensome to investigate a full-factorial sample of possible survivability enhancements. Design-of-experiment techniques are readily applicable to the survivability assessment to mitigate this computational expense (Brynestad and Newberry 1992).

enumerated in the STAR are specified using Likert scaling factors: consequence of threat imposed to the system (C_s), difficulty of an aggressor to impose the threat (D_{agg}), and effectiveness of countermeasures (E_{cm}). Second, a threat risk (*TR*) level is defined:

$$TR = \frac{C_s}{D_{agg} \cdot E_{cm}} \tag{2-1}$$

Third, threat risks are aggregated using likelihood of the threat (*L*) as a weighting factor. Fourth, a lifecycle cost model is created for employment of each countermeasure. Figure 2-4 provides a sample output at this phase of the analysis.

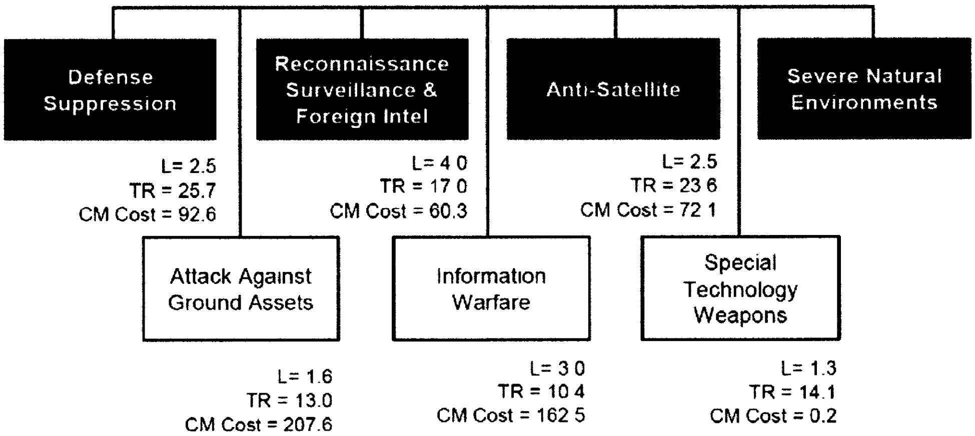
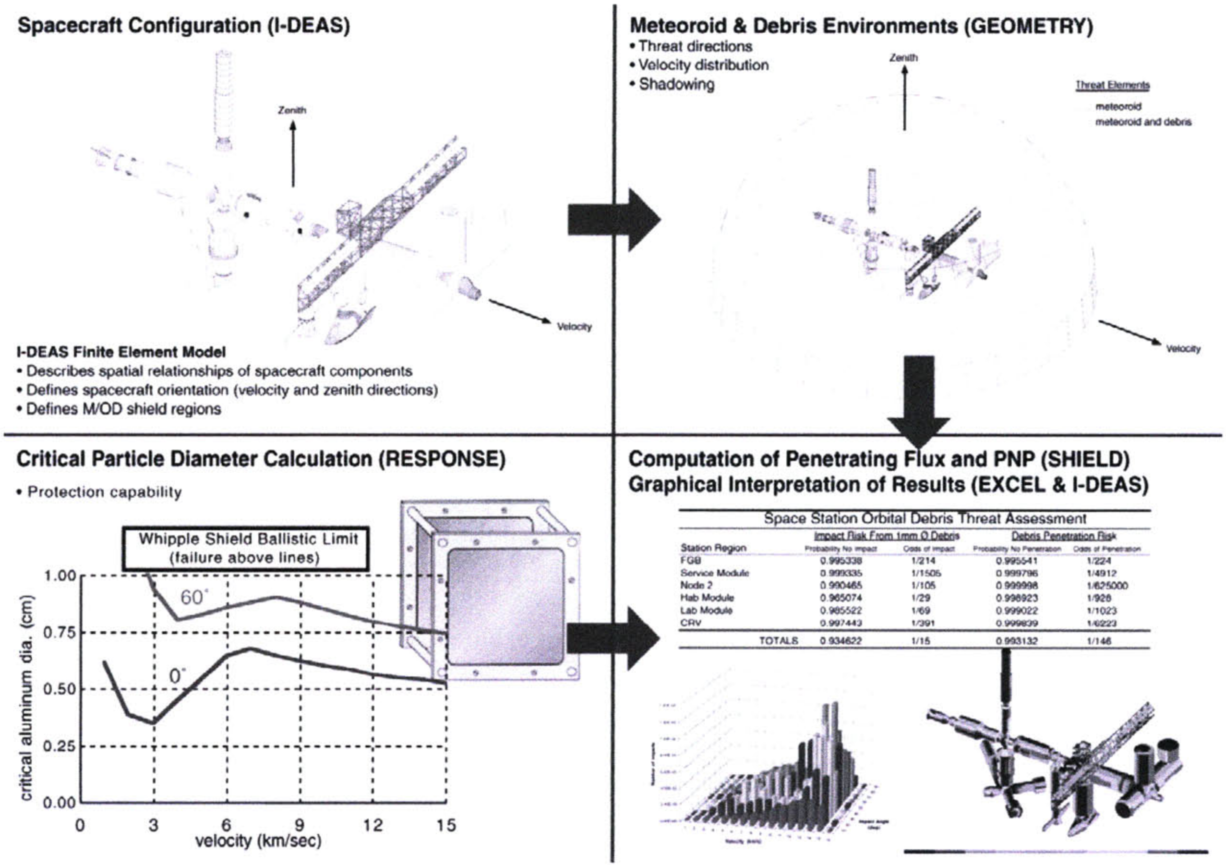


Figure 2-4. Example Threat Evaluation Model (USAF 2005)

Fifth, a baseline *TR* is computed for a design incorporating no countermeasures. In the sixth and final step, linear programming (Hillier and Lieberman 1995) is employed to minimize *TR* for a fixed cost or to achieve a fixed *TR* for minimum cost.

While *The Fundamentals of Aircraft Combat Survivability Analysis and Design* describes survivability engineering only within the domain of combat aircraft, Ball's susceptibility and reduction techniques are applicable to a variety of domains, including satellite protection (Ball and Kolleck 2000). Given its life-critical design requirements and high-susceptibility to orbital debris impacts (due to a surface area of 12,000 m^2 and a 15-year design lifetime), military survivability analysis techniques have regularly been applied to the International Space Station (*e.g.*, Figure 2-5). For example, to improve the likelihood of the International Space Station (ISS) maintaining mission capability following orbital debris penetration, Williamsen *et al.* (1999) used Ball's analytic framework for a three-phased vulnerability assessment: (1) establish ISS failure modes, (2) associate each failure mode with a critical damage level, and (3) determine the probability of orbital debris impacts that induce these critical damage levels. Having developed this vulnerability model, the survivability implications for alternative internal equipment designs and crew operational procedures were examined—identifying minor CONOPS changes that enhanced crew safety following orbital debris penetration.


Spacecraft Configuration (I-DEAS)
Zenith
Velocity
I-DEAS Finite Element Model
• Describes spatial relationships of spacecraft components
• Defines spacecraft orientation (velocity and zenith directions)
• Defines M/OD shield regions
Meteoroid & Debris Environments (GEOMETRY)
• Threat directions
• Velocity distribution
• Shadowing
Zenith
Threat Elements
meteoroid
meteoroid and debris
Velocity
Critical Particle Diameter Calculation (RESPONSE)
• Protection capability
Whipple Shield Ballistic Limit
(failure above lines)
60°
0°
critical aluminum dia. (cm)
1.00
0.75
0.50
0.25
0.00
0
3
6
9
12
15
velocity (km/sec)
Computation of Penetrating Flux and PNP (SHIELD)
Graphical Interpretation of Results (EXCEL & I-DEAS)

Space Station Orbital Debris Threat Assessment

Station Region	Impact Risk From 1mm O Debris Probability No impact	Impact Risk From 1mm O Debris Odds of impact	Debris Penetration Risk Probability No Penetration	Debris Penetration Risk Odds of Penetration
FGB	0.995338	1/214	0.995541	1/224
Service Module	0.999335	1/1505	0.999796	1/4912
Node 2	0.990465	1/105	0.999998	1/625000
Hab Module	0.965074	1/29	0.998923	1/928
Lab Module	0.985522	1/69	0.999022	1/1023
CRV	0.997443	1/391	0.999839	1/6223
TOTALS	0.934622	1/15	0.993132	1/146

Figure 2-5. ISS Debris Threat Assessment (Graves 2002)

Other methodologies take a different approach for determining whether to incorporate survivability features. Rather than seeking to minimize lifecycle cost, Canavan and Teller (1990) use the Nitze criterion to evaluate alternative survivability enhancement features for a space-based ballistic missile defense system. As one of the chief architects of U.S. policy toward the Soviet Union during the Cold War, Paul Nitze advocated that defenses are worth deploying if they are more cost-effective at the margin (*i.e.*, recurring cost of defense is less than the recurring cost of the countermeasures that could be used against the defense). The Nitze criterion is operationalized using cost-exchange ratios (*i.e.*, the marginal cost of defense divided by the marginal cost of countermeasures). Therefore, in examining the Brilliant Pebbles missile defense system,[11] Canavan and Teller use cost-exchange ratios to analyze the strategic interactions between the deployment of an offense (*i.e.*, nuclear attack missiles), the deployment of a defense (*i.e.*, space-based interceptors to collide with the missiles as they leave the atmosphere), countermeasures taken by the offense (*e.g.*, anti-satellite vehicles), and counter-countermeasures taken in turn by the defense (*e.g.*, hardening, evasive maneuvers, decoys). Before accounting for survivability considerations, a Brilliant Pebbles system was shown to have highly-effective cost-exchange ratios with Soviet inter-continental ballistic missiles (ICBMs) when deployed together inside carrier vehicles. However, when accounting for countermeasures,

[11] Described as "the crowning achievement of the Strategic Defense Initiative" by former Lawrence Livermore National Laboratory Director John Nuckolls, the Brilliant Pebbles were a set of non-nuclear watermelon-sized mini-missiles designed to kinetically intercept and kill ballistic missiles in the boost and early mid-course phases of flight.

absenteeism, and cost-effectiveness relative to other defense strategies, Canavan and Teller recommended a distributed singlet deployment (*i.e.*, one interceptor per carrier vehicle) for achieving favorable cost-exchange ratios with the attacker. In addition to informing designers regarding the strategic interaction between a system and its threat environment over time, cost-exchange ratios are also used for survivability tactics optimization. For example, Howard's satellite attrition model (1993) determines an "optimal" decoying strategy based on maximizing the resources expended by an adversary.

2.1.4. Mapping to Related Disciplines

"In time of crisis, there can be uncertainty over whether a particular survivability problem is related to security or to reliability, availability, and fault tolerance" (Neumann 2000).

System properties closely related to survivability include safety, security, and reliability. Given the similarities and interdependencies among these properties (Dotseth 1997), it is important to distinguish among them. To begin, Table 2-1 provides definitions of safety, security, reliability, and survivability found in the literature.

Table 2-1. Disciplines Related to Survivability

reliability	probability of functioning for a prescribed time under stipulated environmental conditions	(Leveson 1995)
safety	freedom from accidents or losses	(Leveson 1995)
security	protection of a system's informational, operational, and physical elements from malicious intent	(Laracy and Leveson 2007)
survivability	capability to avoid or withstand hostile natural and synthetic environments	(USAF 2005)

Safety, "freedom from accidents or losses," is perhaps the discipline most closely linked to survivability in that both disciplines seek to minimize hazards *(i.e.*, system and environmental states which will lead to losses) (Leveson 1995). However, whereas the hazards addressed by system safety encompass both endogenous and exogenous failures (*e.g.*, from operator errors and component failures to flawed software design, dysfunctional component interactions, and unsafe organizational evolution) that emerge from the interaction of a system with its environment (Leveson 2002), the disturbances considered by survivability are all exogenous to the system and consist of both naturally-occurring and man-made hostile environments. In practice, survivability and safety engineers may work closely together. This is particularly true for vulnerability reduction features. For example, the two disciplines cooperated to implement fire protection systems in the fuel tanks of civilian airliners following the loss of TWA Flight 800 (Ball and Atkinson 2006). However, safety and survivability are not always synergistic. For example, while the incorporation of infrared flares in combat aircraft to counter heat-seeking missiles increases survivability, it also reduces system safety by introducing a source of fire (Ball 2003).

Security, "a system property that implies protection of the informational, operational, and physical elements from malicious intent" (Laracy and Leveson 2007), is closely related to survivability in that both are concerned with hostile malevolent environments. However, survivability is distinguished from security by excluding threats internal to the system boundary while including hostile natural environments. In addition, enablers of survivability include not only resistance to attack but also robustness under attack and recovery efforts (Ellison, Fisher et al. 1999).

Reliability, the probability that a component will perform its intended function "for a prescribed time and under stipulated environmental conditions" (Leveson 1995), is primarily concerned with internal component failures while survivability is considered with external system disturbances. Figure 2-6 provides a Venn diagram representation of the relationships among reliability, safety, survivability, and security.

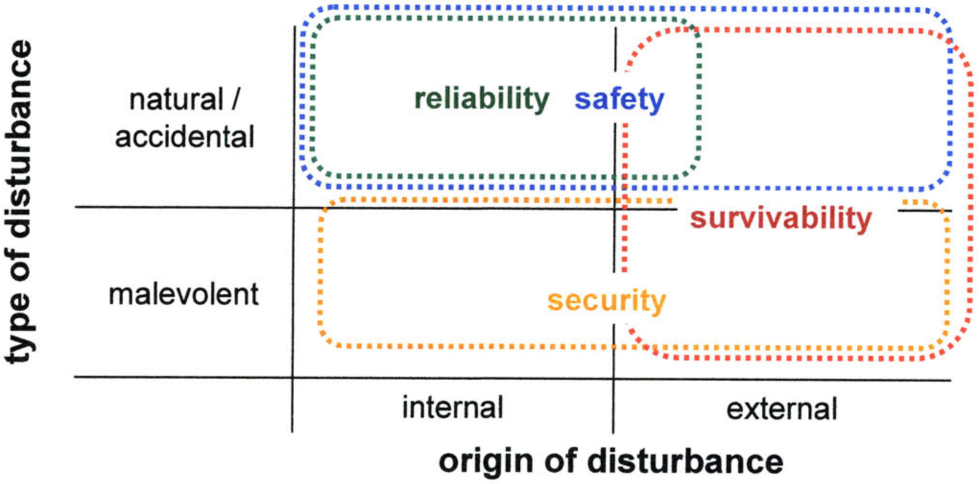


Figure 2-6. Relationships between Survivability and Related Disciplines

Other emerging fields related to survivability include resilience engineering and system assurance. Resilience may be defined as "the ability of a system or organization to react to and recover from disturbances at an early stage, with minimal effect on the dynamic stability" (Hollnagel, Woods and Leveson 2006). Resilience is one enabler of increasing the survivability of systems. Systems assurance has been defined as "the level of confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system" (Baldwin, Komaroff and Croll 2006). While systems assurance is focused on the challenges of validating military software and parts security, given the complex international supply webs characteristic of most modern systems, survivability engineering is focused on the design of systems robust to operational disturbances.

2.2. State-of-the-Practice: Evaluation of Design Alternatives

Having surveyed the practices that characterize modern survivability engineering, existing practices for evaluating design alternatives are now discussed. This more general review is necessary for understanding state-of-the-art system analysis methodologies that might be leveraged within survivability engineering.

Building on the discussion of value-based conceptual design, tradespace exploration, and "-ilities" in Section 1.1, this section examines existing design processes for evaluating and selecting design alternatives with respect to stakeholder needs. Whether structured and explicit or implicit and intuitive, all design teams use a method for selecting concepts for further investigation and development (Ulrich and Eppinger 2004). Given that every system exists to deliver value to stakeholders, a key challenge for any evaluation technique is using subjective stakeholder needs to drive engineering design decisions (Ross 2006). In other words, in presenting alternative designs to a decision-maker and recommending "best" designs for selection, how should analysts establish the link between the value and technical domains?

Decision theory is a field focused on improving how people make decisions (*i.e.*, commitments to courses of action involving an irreversible allocation of resources). The origins of modern decision theory may be traced to the foundational work of von Neumann and Morgenstern (1953) on utility quantification, measurement, and normative axioms. Tang (2006) provides an excellent overview of the three branches of decision theory: the normative, descriptive, and prescriptive schools (Table 2-2). The normative school concerns itself with how decisions ought to be made based upon internal consistency and theoretical adequacy (*e.g.*, expected utility theory). The descriptive school focuses on how decisions are made in reality (*e.g.*, prospect theory), enabling a better understanding of the implications of human biases. The prescriptive school seeks to integrate the theoretical and empirical insights provided by the former two schools to help people make better decisions in practice (*e.g.*, value-focused thinking).

Table 2-2. Summary of Normative, Descriptive, and Prescriptive Theories (Tang 2006)

	normative	**descriptive**	**prescriptive**
focus	how people should decide with logical consistency	how and why people decide the way they do	help people make better decisions prepare people to decide
criterion	theoretical adequacy	empirical validity	efficacy and usefulness
scope	all decisions	classes of decisions tested	specific decisions for specific problems
theoretical foundations	utility theory axioms	cognitive sciences psychology about beliefs and preferences	normative and descriptive theories decision analysis axioms
operational focus	analysis of alternatives determining preferences	prevention of systematic human errors in inference and decision-making	processes and procedures end-end decision life-cycle
judges	"theoretical sages"	experimental researchers	applied analysts

Prescriptive decision theory, also referred to as decision analysis, seeks to "prescribe how a decisionmaker should think systematically about identifying and structuring objectives, about vexing value tradeoffs, and about balancing various risks" (Keeney and Raiffa 1993).[12] A wide variety of decision analysis techniques exist with varying criteria to evaluate system alternatives (Hazelrigg 2003). Each technique has applicability to various stages of product development. Given this thesis' focus on the front-end evaluation of survivability features on stakeholder

[12] Decision analysis is similar to optimization in that both aim to identify an "optimal" choice whose outcome is preferred given an underlying set of objectives. However, while optimization theory deals almost exclusively with search techniques, decision analysis concerns itself with where the objective function comes from and with which constraints it must satisfy (Hazelrigg 2003).

value-delivery (Section 1.1), the subsequent discussion will focus on prescriptive, value-based approaches for conceptual design.

The value-centric perspective is operationalized in conceptual design through the application of decision theory to the engineering design process—making cost-benefit tradeoffs explicit in concept selection (Thurston 1990; Keeney and Raiffa 1993). As a decision aid for multi-criteria assessment of alternatives, multi-attribute utility theory (MAUT) provides a construct for assessing values and subjective probabilities of individuals in the presence of uncertainty due to risk (Dyer et al. 1992). Founded upon mathematical theory for utility models (Keeney and Raiffa 1993), MAUT's logical consistency is coupled with a variety of assessment techniques that address the limited cognitive abilities of decision-makers. As prescriptive theory, MAUT's potential is implicitly recognized by descriptive theories that characterize human decision-making (in the absence of such methodological structure) in terms of heuristics and biases (Tversky and Kahneman 1974) as well as bounded rationality (Gigerenzer and Goldstein 1996; Simon 1996).

2.2.1. Trade Studies in Conceptual Design

Trade studies are analyses that evaluate a range of design options in terms of costs and benefits. According to the *NASA Systems Engineering Handbook* (2007), trades studies are used to propose and determine the feasibility of design alternatives for a given mission. Systems engineering texts recommend using legacy systems, new technologies, innovative concepts, and stakeholder-suggested systems to enumerate the set of design alternatives to be evaluated in a trade study (Kossiakoff and Sweet 2003).

Despite the extremely negative cost, schedule, and performance implications of making poor design decisions during conceptual design (Section 1.1.2), development of systems involving new technologies does not typically involve a broad, systematic exploration of design alternatives (McManus and Warmkessel 2004). In practice, the intuition of experienced designers is usually consulted in the pursuit of a feasible solution or solutions (*i.e.*, designs within the acceptability range of stakeholder cost and benefit), (Maier and Rechtin 2002). Typically, the unavailability of resources for consideration of a multitude of options compel design teams to establish favorite baseline "point designs" from which small perturbations are examined in an analysis-of-alternatives (Ross and Hastings 2005). This approach of rapidly converging and optimizing on a conceptual design is susceptible to identifying locally optimal designs that provide only a vague picture of the complexity of the broad space of possible designs (McManus and Warmkessel 2004).

Figure 2-7 illustrates four levels of trades that can be conducted during conceptual design: (1) local point solution trades, (2) examination of a small number of point designs in an analysis-of-alternatives, (3) multi-objective optimization to identify designs along the Pareto front, and (4) full tradespace exploration. Each type of trade is identified within a notional tradespace, *i.e.*, the space spanned by an enumerated set of design variables, X_i, that specify design alternatives. While choosing to do a *Level 1* design trade requires the least effort, incomplete understanding of the broader tradespace may lead to selection of a suboptimal solution (*i.e.*, a dominated point lying in the interior region of the tradespace). A recommended improvement to local point solution trades is to conduct a *Level 2* analysis-of-alternatives (AoA) to assess the alternatives in different regions of the tradespace (Herscovitz and Barnett 2007). However, there is no assurance that the relatively small number of designs in the AoA are non-dominated solutions.

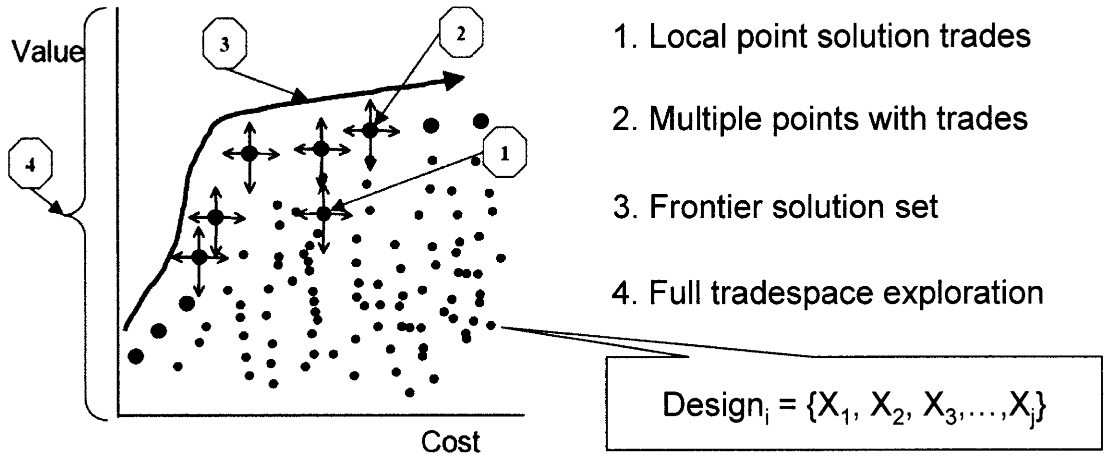

Value
Cost
1
2
3
4
1. Local point solution trades
2. Multiple points with trades
3. Frontier solution set
4. Full tradespace exploration
$\text{Design}_i = \{X_1, X_2, X_3, \ldots, X_j\}$

Figure 2-7. Different Types of Trades within the Design Space (Ross and Hastings 2005)

Extending traditional trade studies, which typically consider a small number of alternative designs, multi-objective optimization and tradespace exploration leverage computer-based parametric models and simulations to compare hundreds or thousands of potential architectures. If full tradespaces are deemed too large to enumerate, analyze, and compare all possible alternatives, a variety of optimization techniques (*e.g.*, Taguchi, heuristic, gradient, univariate) may be used to approximate the Pareto front in a *Level 3* trade study (Jilla 2002). Finding the Pareto frontier solution set enables explicit value trade-offs to be made among design alternatives. However, restricting the trade study to Pareto-efficient designs limits the breadth of understanding to be gained by mapping the decision-maker preference structure onto the entire design space. For example, without having enumerated and evaluated designs lying in the interior of the tradespace, it is not possible to investigate the sensitivity of the "optimal" designs to changes in the objective function. Therefore, a *Level 4* exploration of the tradespace considers dominated solutions as well as the Pareto front (Ross and Hastings 2005).

2.2.2. Emerging Method: Multi-Attribute Tradespace Exploration

Multi-Attribute Tradespace Exploration (MATE) is a conceptual design methodology that applies decision theory to model and simulation-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.[13] 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. To date, MATE has been applied to over a dozen (mostly aerospace) systems and utilized in research examining requirements generation (Diller 2002), policy uncertainty (Weigel 2002), space system architecting and design (Ross 2003), concurrent engineering (Stagney 2003), spiral development (Roberts 2003), evolutionary

[13] The solution-generating aspect distinguishes MATE from traditional decision analyses techniques which focus only on the evaluation step.

acquisition (Derleth 2003), modularity (Shah 2004), orbital transfer vehicle design (Galabova 2004), and value robustness (Ross 2006). Figure 2-8 summarizes the MATE process.

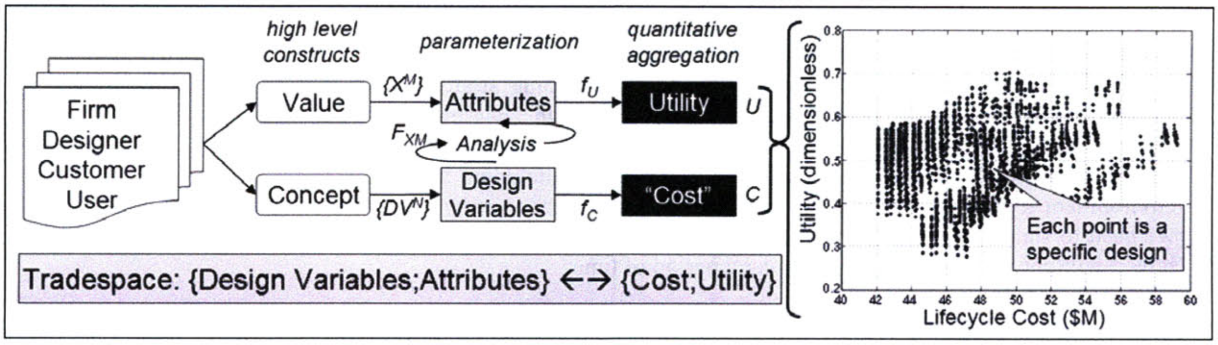


Figure 2-8. Multi-Attribute Tradespace Exploration (MATE) (Ross, Hastings et al. 2004)

Ross (2003) provides a detailed description of the 48 steps comprising a full MATE study. At a high level, the process consists of three general phases: need identification, design alternative enumeration, and design alternative evaluation. In the first phase, the mission needs and preferences of a decision-maker are defined and specified with attributes (*i.e.*, decision-maker-perceived metrics that measure how well decision-maker-defined objectives are met). Attributes and their associated utility curves and multiplicative weighting factors are elicited through formal utility interviews with decision-makers. Single-attribute utility curves are typically aggregated using a multiplicative utility function (*i.e.*, a dimensionless metric of user satisfaction ranging from 0, minimally acceptable, to 1, highest of expectations).

In the second phase, the attributes are inspected and various design variables are proposed. (Design variables are 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—explicitly links the value and technical domains of a system.

In the third phase, physics-based models are developed to evaluate the lifecycle cost and utility of the designs under consideration. To assess the full-factorial sampling of the design space, parametric computer models are used to transform each design vector into attribute values against which utility functions can be applied. Following a MATE analysis, a limited number of Pareto-efficient designs may then be matured in a concurrent engineering environment. 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.

One of the advantages of conducting a *Level 4* tradespace exploration using MATE over a *Level 3* search of the Pareto front using traditional optimization techniques is that the sensitivities of the design alternatives to changing decision-maker needs, operational (threat) environments, and technological developments, can be explored. As discussed in Section 1.1.4, the lifecycle system properties known as the "-ilities" (*e.g.*, flexibility, robustness, survivability) are increasingly regarded as critical for delivering sustained stakeholder value. A recent Air Force/Lean Aerospace Initiative report on systems engineering (Rhodes 2004) articulates this need:

> ...we need to understand what makes an architecture robust, and this is not well understood today... a robust architecture must be developed against a list of "threats", scenarios, and environments rather than for a specific point design. A challenge we face is developing strategies and methods for insulating the architecture against dramatic change- for example, through layering or modularity. There is a need to separate elements that change rapidly from those that are static- adjusting for "clockspeeds...we need to be able to envision where the system will be in 20+ years, including the nature of future missions and the environment it will need to operate in. And, as systems are moving toward more collaborative SoS/FoS, we need to simultaneously define the context in which the current system will operate, as well as defining how it will play in multiple contexts over a period of time.

Despite general agreement on their importance, the "-ilities" are neither well-defined nor easily evaluated in isolation. Two key challenges make the "-ilities" difficult to represent in a classic tradespace: (1) representation of temporal properties in a static construct (2) axiomatic restrictions on the incorporation of the "-ilities" in attribute sets (*i.e.*, attributes need to be perceived as independent, yet the "-ilities" are defined by attribute performance over time).[14]

Ross (2006) operationalized six "-ilities" (*i.e.*, changeability, flexibility, adaptability, scalability, modifiability, and robustness) for assessment in trade studies through the incorporation of time-dependent context variables in MATE. In a dynamic MATE study, network analysis is applied to a series of temporally-linked tradespaces, enabling the quantification of "-ilities" as decision metrics across design alternatives. In order to incorporate time into traditionally static cost-utility tradespaces, Epoch-Era Analysis (Figure 2-9) is employed whereby a system lifecycle or "era" is modeled as a set of discrete epochs. Equivalent to short-run analysis in economics, a given epoch defines a scenario in which constraints, design concepts, available technology, and articulated attributes remain fixed.

[14] The "-ilities" cannot be incorporated as traditional attributes in MATE due to three theoretical inconsistencies: lack of decomposability, lack of perceived independence, and redundancy. Since their definition is related to changes in system form or function, they are quantitatively dependent upon other objective function variables. Tradespace studies typically look at the relation between function and/or form and resulting system performance in terms of system objectives. The performance in an aggregated, multi-objective space is dependent on performance in each of the single objectives. In choosing an appropriate aggregation technique, it is important not to double-count the single objective performances. Aggregating "-ilities", which by definition are measures of the ability to maintain attributes under changing conditions, into a multi-attribute objective function will run into the problem of double-counting. An active area of research is seeking to formulate an appropriate basis for aggregating "-ilities" with other system attributes. In the meantime, the "-ilities" will remain disaggregated and their impact in a tradespace study assessed independently (McManus, Richards et al. 2007).

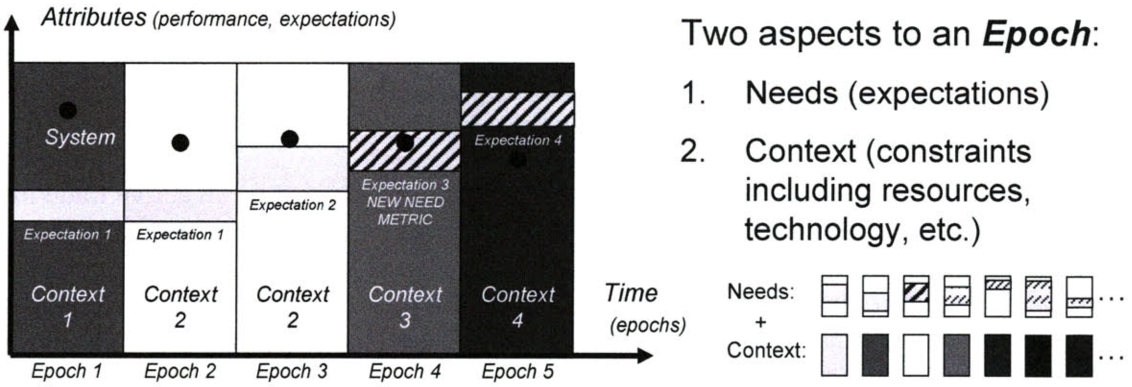


Figure 2-9. Epoch-Era Analysis

Just as a movie reel approximates motion by stringing together multiple static pictures in quick succession, dynamic MATE strings together multiple static tradespaces over time to approximate dynamic system contexts and expectations. System states may be represented within an epoch using a network tradespace. In the limit that the design vectors in the tradespace represent all meaningful system states, a dynamic model may be approximated within the tradespace as transitions between design vectors over time. An accessibility matrix specifies the ability of one design to transition to another, and a transitions rules matrix specifies the time and cost incurred for a given transition. To evaluate a system's robustness to change, Ross introduced the Pareto Trace number, the frequency with which a particular design appears in the Pareto front of enumerated tradespaces. System changeability is measured by Filtered Outdegree, the number of potential transition paths available to a design, filtered by acceptable cost for change by a particular decision-maker (Ross and Hastings 2006).

2.3. Limitations of Existing Survivability Methods

> *"The current state of practice in survivability and security evaluation tends to treat systems and their environments as static and unchanging. However, the survivability and security of systems in fact degrade over time as changes occur in their structures, configurations, and environments, and as knowledge of their vulnerabilities spreads...." (Ellison, Fisher et al. 1999)*

Several opportunities to improve the practice of survivability engineering (Section 2.1) may be identified when analyzing the discipline from the perspective of dynamic, value-driven tradespace exploration (Section 2.2). This section discusses five limitations of existing survivability methods: (1) treatment of survivability as a constraint rather than an active trade in the design process, (2) static nature of system threat assessment reports despite changing operational environments, (3) assumption of path-independent disturbance encounters, (4) limited scope of survivability design and analysis, and (5) inability to consider alternative value-delivery mechanisms.

2.3.1. Treatment of Survivability as a Constraint

> *Designing an air vehicle to maximize mission effectiveness subject to cost and survivability constraints for a fixed operational situation is the classic cost-effectiveness criterion... "*
> -pg. 90 of Future Air Force Needs for Survivability, Air Force Studies Board, (NRC 2006)

The first limitation, the treatment of survivability as a constraint rather than an active trade in the design process, restricts the design space available to designers before conceptual design has even begun. While specifying a minimum level of survivability may be appropriate for the design of piloted aircraft, the wisdom of specifying survivability as a constraint on the design of unmanned aerial vehicles and satellites *a priori* is less clear because survivability versus quantity trade-offs may reveal more valuable system designs (Jeffcoat 2003). Since the beginning of the space era, incorporating survivability as a parameter in system-level trade studies (*e.g.*, with lifecycle cost and mission utility) has proven to be challenging. The first reconnaissance satellite program, CORONA,[15] provides a revealing example (Wheelon 1997). Fearing the vulnerability of CORONA satellites to attack by the Soviet Union, a wide range of defensive measures were examined, including inflating and deploying decoy balloons and orbit-adjust maneuvers (Wheelon 1965). However, CORONA protection was never implemented because of the payload weight required, mutual forbearance towards space warfare (once the Soviets developed their own reconnaissance capabilities), and an inability to trade film weight (*i.e.*, performance) with survivability measures.

2.3.2. Static System Threat Assessment Reports

The second limitation of existing survivability methods is attributed to the static nature of the System Threat Assessment Report. Upheld as the authoritative description of a system's operational hazards and the document from which survivability requirements are derived, the STAR suffers from the potential for obsolescence before system end-of-life. For example, the life span of a combat aircraft from program inception (when the STAR is issued) to removal from service might stretch beyond 50 years (Ball 2003). A similar disconnect exists for space system design given the long gestation period and operational life of satellites. Furthermore, practitioners admit that "selected operational scenarios are not likely to truly represent future conflicts," "unanticipated technological developments will affect combat operations," and "adversaries in real conflicts will adapt to our capabilities in unanticipated ways" (Anderson and Williamsen 2007). Given that survivability is an inherently dynamic property (Ellison, Fisher *et al.* 1999), it is troubling that current methods rely on static assumptions.

Utilizing cost-exchange ratios for survivability analysis provides a means for modeling the strategic interaction between attackers and defenders over the lifecycle of a system. However, the Nitze criterion does have limitations when applied to the more general challenge of determining whether to build a defensive system. In particular, cost-exchange ratios may not be valid if the value of a particular dollar spent on defense is not conserved across actors. This disparity may have existed during the Cold War given the larger size of the U.S. economy relative to the Soviet Union; and this disparity certainly exists today given the many asymmetric threats to U.S. security.

[15] The CORONA program refers to a series of 145 photo reconnaissance satellites launched to low Earth orbit between 1960 and 1972, providing the "backbone of US intelligence capability for twelve precarious years" (Wheelon 1997).

2.3.3. Assumption of Independent Disturbance Encounters

Survivability analysis is appropriately founded upon probabilistic risk assessment (PRA) given that the outcome between a system and a disturbance environment is not deterministic. However, many of the underlying assumptions made in applications of PRA are frequently inappropriate. For example, Leveson (1995; 2002) documents several limitations of PRA in its application to system safety. These limitations are even more pronounced in survivability assessments. The fundamental issue with PRA is that, although it is intended as a systematic methodology to measure risk in complex systems, two of its key underlying assumptions (in practice) may not hold for complex systems: that all probability distributions are known and that system components are independent (Harper, Thornton and Szygenda 2007). In *Normal Accidents*, Perrow (1999) finds that failures may also arise from unanticipated, dysfunctional interactions among components and then subsequently be exacerbated by the rapid propagation of local failures due to tight coupling in complex systems. These findings are consistent with the system safety literature which points out additional flaws, such as the limits of redundancy given common-cause failures (Pate-Cornell, Dillon and Guikema 2004); problems with using historical data as a representative sample of current failure probabilities; and narrow focus of PRA on immediate physical failures (Leveson 2002).

Criticisms of the simplifying assumptions of PRA in the safety engineering literature are certainly valid for existing survivability engineering methods (Ball 2003) that assume linear, independent weapon encounters despite the existence of nonlinear, dependent failure modes. For example, systems degraded from an initial disturbance will be more vulnerable to a subsequent disturbance (and potentially more susceptible as well in the case of an intelligent adversary). Eliminating path dependencies in the calculation of system susceptibility, vulnerability, and recoverability abstracts much of the necessary complexity in survivability analysis.

2.3.4. Narrow Scope of Survivability Design and Analysis

The fourth limitation is the limited scope of survivability design and analysis. Since survivability engineering was established as a formal design discipline in the 1960's, a tremendous amount of progress has been made to improve the survivability of individual elements in aerospace system architecture (Nordin and Kong 1999; Paterson 1999).

Less progress has been made, however, at the architecture-level where systems tend to evolve in an ad-hoc manner—accommodating constraints from legacy systems and forming temporary coalitions to support emergent missions. More generally, architecting for survivability is a poorly understood, socio-technical issue, increasingly relevant to all engineering systems. For example, despite the recognized criticality of low-probability, high-consequence events (Leveson 1995; Sheffi 2005), modeling these events, evaluating the benefits of protective measures, and internalizing the role of operational behavior, human factors, and supporting infrastructures is the subject of ongoing research (Leveson et al. 2004). Furthermore, existing models of highly survivable system architecture from the Cold War (*e.g.*, Nuclear Command and Control System) are not readily applied given the virtually unlimited resources allocated to such systems in that era. In analyzing the shortcomings of current methods for the specification, development, procurement, operation, and maintenance of systems and networks with critical survivability requirements, Neumann (2000) succinctly describes the state of the discipline:

> *"The currently existing evaluation criteria frameworks are not yet comprehensively suitable for evaluating highly survivable systems and networks.... There is almost no experience in evaluating systems having a collection of independent criteria that might contribute to survivability... "*

In the space domain, the need for a comprehensive survivability architecture is particularly critical given the interdependencies among spacecraft, ground stations, and communications links (Shellans and Matoush 1992). However, existing design and analysis methodologies focus on survivability at the satellite-level rather than higher levels in the system architecture (*e.g.*, Air Force mission area).

2.3.5. Lack of a Value-Centric Perspective

The fifth limitation of existing survivability design methodologies is the lack of a value-centric perspective. Success of a system before, during, and after a disturbance is dependent on how much functionality it delivers to its stakeholders, not strictly the physical integrity of system components. Unless the stakeholders care about the mechanism by which value is delivered, which is rare, the system is free to deliver value by many possible means. This is particularly useful for resolving survivability issues when original value delivery mechanisms may be blocked due to a disturbance. Utilization of value as a unifying metric also enables evaluation of protection measures at various levels in the system architecture (*e.g.*, explore cost-benefit tradeoff of increasing hardness of individual satellite *vis-à-vis* investing in reconstitution capability). Taking the value-centric perspective, system designers are freed to consider multiple paths to achieve the same value delivery (Ross 2006).

2.4. Problem Statement

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

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

Given the limitations of existing survivability design methods for aerospace systems (*i.e.*, treatment of survivability as a constraint on design, static system threat assessment reports, assumption of independent weapon encounters, limited scope, and exclusive focus on physical integrity), there is a need for a design method that (1) incorporates survivability as an active trade in the design process, (2) captures the dynamics of operational environments over the entire lifecycle of systems, (3) captures path dependencies of system survivability to disturbances, (4) extends in scope to architecture-level survivability assessments, and (5) takes a value-centric perspective to allow alternative value-delivery mechanisms in the tradespace. Recent research on how decision-makers can recognize and evaluate dynamically relevant designs, including Multi-Attribute Tradespace Exploration (Ross, Hastings *et al.* 2004) and Epoch-Era Analysis (Ross 2006), offers a theoretical foundation for the development of an improved design methodology for survivability.

3. Defining Survivability for Engineering Systems

This chapter addresses the first of the four research questions introduced in Section 1.3.2.

1. What is a dynamic, operational, and value-centric definition of survivability for engineering systems?

The objective of this chapter is to conceptualize and operationalize survivability for subsequent analysis. Existing survivability metrics vary both within and across domains and are traditionally calculated with specific operational scenarios in mind. Therefore, a general definition of survivability is a critical first step towards the development of a general survivability analysis methodology.

Three sections comprise this chapter. First, the introductory discussion of the "-ilities" in Section 1.1.4 is extended and a conceptual framework for relating survivability to the other "-ilities" is described (Section 3.1). Second, existing definitions of survivability are surveyed and a general definition of survivability is introduced (Section 3.2). Third, the construct validity of existing survivability metrics to this general definition is examined, and the survivability metrics of *time-weighted average utility loss* and *threshold availability* are proposed (Section 3.3).

3.1. "-ilities" Framework

"-ilities" may be defined as temporal system properties that specify the degree to which systems are able to maintain or even improve function in the presence of change.[16] The "-ilities", including survivability, have in common the concept of "change." It is the "what is changing" aspect that can be used to differentiate among the "-ilities". System success may be defined in relation to three primary factors: the expectations on the system (*Needs*), the system form (*System*), and the development and operational environment of the system (*Context*). This definition parallels Simon's conceptualization of engineering which "involves a relation among three terms: the purpose or goal, the character of the artifact, and the environment in which the artifact performs" (Simon 1996). The dynamics among these three factors determine the perceived success of the system. The "-ilities" of a system address the ability of the system to cope with changes in these factors.

Assuming a system-centric perspective, the "-ilities" provide a strategy for *system* change in response to changes in *needs* and *context*. Changes in context are usually external constraints on the system: it must operate successfully in the new context. Changes in needs may include increased expectations on the system (*e.g.*, a demand for higher levels of the same service or service in more locations) or changes in the metrics of success (*e.g.*, some new function is demanded of the system). To be successful, the system must deliver more, less, or different, value as needs change. It is important to recognize that a system designer typically only has influence over a system's form; the form as mediated by the operational environment determines the system's performance, and if the performance meets the expectations, the system is perceived to be successful and hence deliver value to its stakeholders.

[16] This excludes some non-operational "-ilities", such as manufacturability, that affect the design of the system but not its operation.

The variety of "-ilities" in the literature need to be clarified in a structured framework in order to be useful to system analysts. Given that changing needs, context, and system states are the common threads which tie the "-ilities" together, one way of taxonomically organizing the "-ilities" is with a three-dimensional "-ilities Space" (Figure 3-1) with the parameter of time. The three factors that can change over a system lifetime are the *system* itself (*i.e.*, an object or group of objects in physical space, representing hardware designs but also more abstract parts of the system such as software or operating procedures or connections between the parts); the *needs* of stakeholders (*i.e.*, a perceived abstraction in the minds of the stakeholders, often represented by utilities), and the *context* (*i.e.*, the development and operational space outside of the system boundary, represented as constraints, both explicit and embedded in the modeling of the physical reality in which the system operates). Note that these are not single-dimensional axes *per se*; only in an extremely simple case (of one monotonic variable on each axis) could one actually plot anything quantitatively in this space. For a given context and system state, the *performance* is determined in the same units or language as the *needs*. If the performance exceeds the *expectation* level of the relevant stakeholders (*i.e.*, enough needs are met) then the system is considered successful.

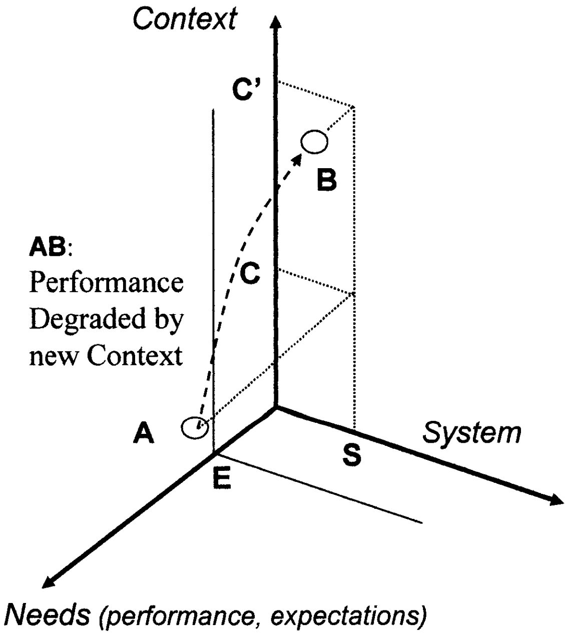


Figure 3-1. "-ilities Space"

In Figure 3-1, a system with configuration S operates in a context C. Its performance is determined and plotted along the Needs axis such that the system's position in the space is A. This point is in front of the iso-needs plane determined by the expectations of the users, E, so the system is successful. However, if the context changes to C', the performance of the unmodified system is now determined to be B, which does not meet expectations. The system's performance has been unacceptably degraded by the change in context. It is possible to imagine that, over the lifetime of a system, it will trace a trajectory through this space. A successful system will perform at or above the (possibly changing) user expectations throughout its lifetime.

The "-ilities Space" is useful for abstract thinking about the interactions between shifting needs, contexts, and system configurations over time, and may be used to distinguish between and among the "-ilities" themselves.[17] Having characterized "-ilities" as temporal system properties describing the ability of systems to navigate changes in the technical, environmental, and value domains, a conceptualization of survivability is introduced within this framework.

3.2. Conceptualizing Survivability

3.2.1. Domain-Specificity of Existing Definitions

Definitions for survivability vary across the biological, network security, and aerospace and defense domains (Table 3-1). While the "continuation of life" is a simple, clear definition for the life sciences, there is less clarity in defining survivability for engineering systems. Formerly proposed metrics for survivability include: the range of environments within which an entity remains operational, the disturbance threshold above which an entity will cease to function, the degree to which performance remains following a disturbance, and the time required to restore health following a compromising disturbance. A general definition of survivability is a necessary precursor to the development of a design process for survivability that may be applied across domains.

In the 1960's, the U.S. Department of Defense (DoD) formally defined survivability as "the system capacity to resist a hostile environment so that it can fulfill its mission" (MIL-STD-721, DOD-D-500.3). Numerous other definitions and evaluation criteria are noted in Table 3-1. Traditionally calculated by military planners with specific operational scenarios in mind, survivability is often defined subjectively—dependent not only on susceptibility and vulnerability assessments (Section 2.1.3)—but also on the range and breadth of proposed missions, threat levels, and the availability of supporting assets within missions (Hall 2004).

Even within domains, there are definitional discrepancies. For example, survivability of communications networks has been defined in terms of reliability as the "probability of retaining connection between representative pairs of nodes" (Al-Noman 1998), in terms of the capability of a system "to perform required functions at a given instance in time after a subset of components becomes unavailable" (Yurick and Doss 2002), and in terms of regeneration as the "degree to which systems recover from attacks" (Moitra and Konda 2000).

[17] McManus, Richards, Ross, and Hastings (2007) define several "-ilities" within the "-ilities Space", including flexibility, adaptability, robustness, versatility, scalability, and modifiability.

Table 3-1. Spectrum of Survivability Definitions

domain	definition/criteria	reference
aircraft	capability of a system and crew to avoid or withstand a man-made hostile environment without suffering an abortive impairment of its ability to accomplish its designated mission	(DoD 2002)
	capability of an aircraft to avoid and/or withstand a man-made hostile environment	(Ball 2003)
biology	environmental fitness of organisms; evolutionary longevity of species to natural selection	(Darwin 1859)
	continuation of life	(Webster 2008)
telecommunications	percentage of stations both surviving the physical attack and remaining in electrical connection with the largest single group of surviving stations	(Baran 1964)
	property of a system, subsystem, equipment, process, or procedure that provides a defined degree of assurance that the named entity will continue to function during and after a natural or man-made disturbance; qualified by specifying the range of conditions over which the entity will survive, the minimum acceptable level or post-disturbance functionality, and the maximum acceptable outage duration	(NTIA 1996)
	probability of retaining connection between representative pairs of nodes	(Al-Noman 1998)
	capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents	(Ellison, Fisher et al. 1999)
	ability to satisfy and to continue to satisfy critical requirements in the face of adverse conditions; defined with respect to the set of adversities that are supposed to be withstood	(Neumann 2000)
	ability of a system to perform required functions at a given instant in time after a subset of components become unavailable	(Yurick and Doss 2002)
	capability of an information system to fulfill its mission by preserving essential services, even when systems are penetrated and compromised	(Moore and Ellison 2003)
spacecraft	physical means of making satellites survivable against threats and the cost effectiveness ratios, or ratios of attack to defense costs, for the resulting platforms and constellations	(Canavan 1991)
	ability of a space system to perform its intended function after being exposed to a stressing natural environment or one created by an enemy or hostile agent	(Nordin and Kong 1999)
	capability of a system to avoid or withstand hostile natural and manmade environments without suffering abortive impairment of its ability to accomplish its designated mission	(USAF 2005)

3.2.2. General Definition of Survivability

Given that all systems exist to deliver value, a general definition will achieve domain-neutrality by defining survivability in terms of value. Furthermore, as an emergent system property that reveals itself over time, it is critical that the temporal aspects of survivability be internalized.

These principles and the desire for a quantitative formulation guided the development of the following definition.

> *Survivability is the ability of a system to minimize the impact of a finite-duration disturbance on value delivery, achieved through (I) the reduction of the likelihood or magnitude of a disturbance, (II) the satisfaction of a minimally acceptable level of value delivery during and after a disturbance, and/or (III) a timely recovery.*

As discussed in Section 1.1.2, a value-centric conceptualization of survivability is desirable during the conceptual design of systems because it provides a fundamental metric for relating system properties to desired stakeholder outcomes. Taking the value-centric perspective during conceptual design empowers decision-makers to rigorously evaluate and compare different system concepts in the technical domain using a unifying set of attributes in the value domain. The ability to consider multiple system concepts using a unifying set of attributes is particularly useful for survivability when original value delivery mechanisms may be blocked by a disturbance.

In addition to conceptualizing survivability as a value-centric property, it is also important to recognize the inherently dynamic nature of survivability. 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).

Recognizing survivability as a dynamic system property informs three general survivability design strategies over the lifecycle of a disturbance. Type I survivability, *susceptibility reduction*, is the reduction of the likelihood or magnitude of a disturbance. Type II survivability, *vulnerability reduction*, is the minimization of the disturbance-induced losses on value delivery. (Systems that are Type II-survivable may exhibit graceful degradation in which at least minimal functionality is maintained in the event of disturbance-induced losses. The reduced magnitude and rate of value losses in systems that degrade gracefully is in contrast to fragile systems where small disturbances may cause total system failure.) Type III survivability, *resilience enhancement*, is the maximization of the recovery of value-delivery within a permitted recovery time. Figure 3-2 provides a notional illustration of Type I, Type II, and Type III survivability in terms of value delivery over time [$V(t)$].

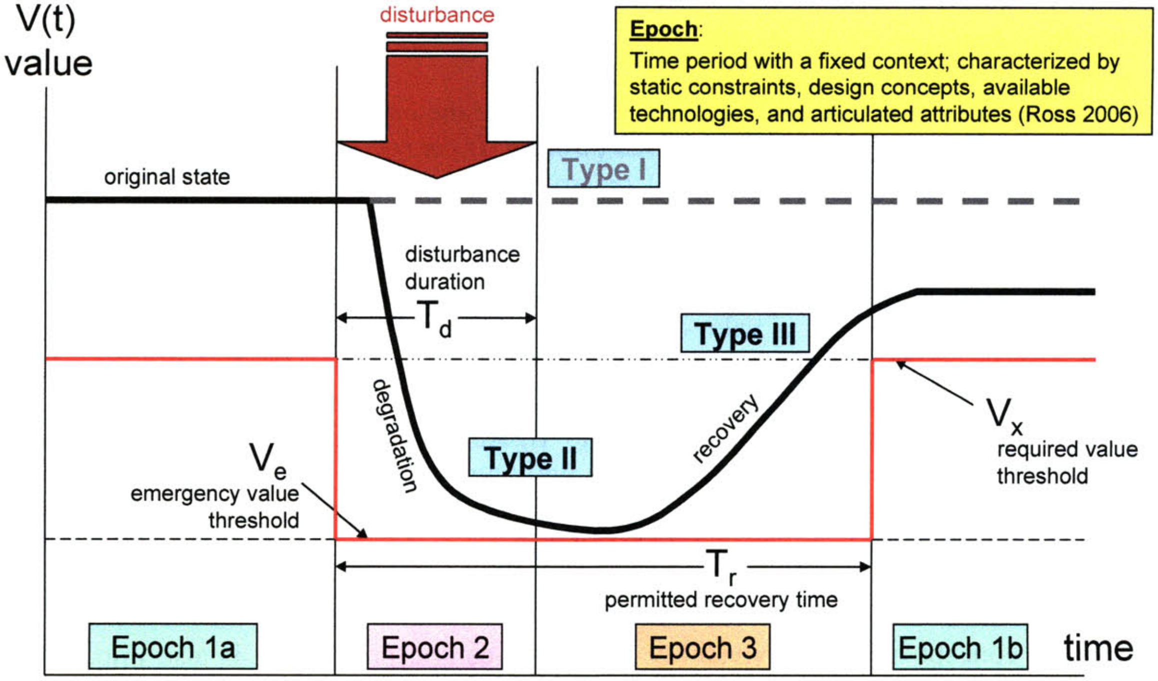


Figure 3-2. Conceptualization of Survivability

In Figure 3-2, time is discretized across four epochs, periods of a fixed environmental context and static stakeholder needs (Ross, Rhodes and Hastings 2008). Following successful value delivery during baseline environmental conditions and stakeholder expectations (Epoch 1a), the system experiences a finite disturbance that degrades performance. Value delivery expectations on the system may be lower during the disturbance (Epoch 2) and in the time period immediately following (Epoch 3) before returning to baseline expectations (Epoch 1b). Type I survivability, depicted as a dashed horizontal line, is achieved if the disturbance fails to reduce *V(t)* below the required value threshold [V_x] over all of the Epochs. In order to determine whether the system is Type II or Type III survivable, two additional factors must be defined: the minimum acceptable value to be delivered during and immediately after the disturbance [V_e] and the permitted recovery time elapsed past the onset of the disturbance [T_r]. In Figure 3-2, the solid line depicts a system achieving Type II survivability by maintaining *V(t)* at a level above V_e during Epoch 2 and Epoch 3. The solid line also depicts a Type III-survivable system as *V(t)* recovers to a level above V_x within T_r. In general, by defining *t'* as the time of the beginning of Epoch 2 (*i.e.*, beginning of a disturbance encounter), three conditions are required for the achievement of survivability:

1. $V(t)\big|_{Ep1} \geq V_x\big|_{Ep1} \quad when \quad t < t'$
2. $V(t) \geq V_e \quad when \quad |t - t'| \leq T_r$
3. $V(t)\big|_{Ep1} \geq V_x\big|_{Ep1} \quad when \quad |t - t'| > T_r$

This general definition conceptualizes survivability as the relationship between stochastic system value trajectories and changing stakeholder expectations across nominal and disturbed environmental states. The conceptualization is consistent with both engineering practice and concepts of risk held by executives. In engineering practice, temporary outages of functionally during and immediately following disturbances are frequently permitted such as with information systems following natural disasters (Ellison, Fisher et al. 1999) and with interplanetary spacecraft entering safe mode following anomalies (Bayer 2007). The case of direct broadcast TV is another example in which an outage time of 0.3% of the year (*i.e.*, 25 hours) is permitted due to Ku-band rain attenuation (Pratt, Bostian and Allnutt 2003). To meet this annual T_r, DIRECTV communication links are design with a margin of 5.7 decibel (Figure 3-3).[18]

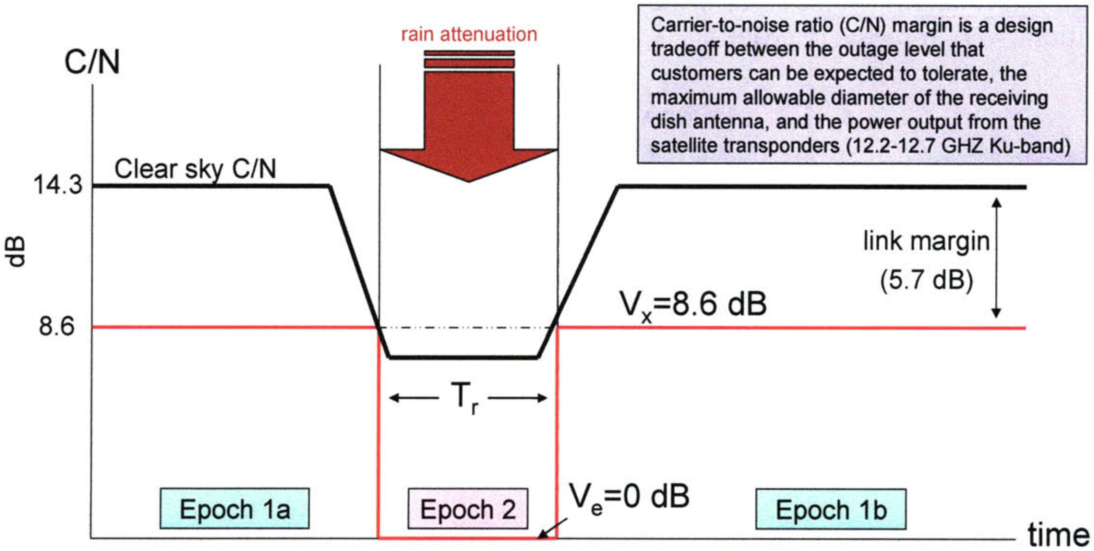

rain attenuation
C/N
Carrier-to-noise ratio (C/N) margin is a design tradeoff between the outage level that customers can be expected to tolerate, the maximum allowable diameter of the receiving dish antenna, and the power output from the satellite transponders (12.2-12.7 GHZ Ku-band)
Clear sky C/N
14.3
dB
link margin
(5.7 dB)
V_x=8.6 dB
8.6
T_r
Epoch 1a
Epoch 2
V_e=0 dB
Epoch 1b
time

Figure 3-3. Survivability Example: Direct TV

The decision analysis literature also supports the conceptualization of survivability in Figure 3-2, particularly V_x and V_e. In analyzing managerial perspectives on risk, March and Shapira (1987) observe that there are two focal values in executive-level decision-making: a target level of performance and a survival level. With these two reference points, the outcome space is partitioned into three parts: success, failure, and extinction.[19] March and Shapira's two focal values are analogous to the critical value thresholds of V_x and V_e and their outcome space partitioning aligns with the potential trajectories of $V(t)$.

[18] Given that recovery from rain attenuation is instantaneous, the permitted recovery time is assumed to be zero and Epoch 3 is excluded from Figure 3-3.

[19] March and Shapira (1987) further observe prospect theoretic behavior around these critical value thresholds: managers barely above the performance target are risk averse while managers below (or expected to be below) the performance target are risk taking.

3.2.3. Distinguishing Between Survivability and Robustness

Due to the confusion associated with the "-ilities" definitions and relationships (McManus and Hastings 2006), it is helpful to discuss the similarities and differences that survivability has with a closely related "-ility": robustness. Both survivability and robustness are measures of the ability of systems to reduce the sensitivity of their outputs to changes in the environment. Using the "-ilities Space" framework (Figure 3-1), Figure 3-4 depicts a sample robust system (AB) as maintaining performance and meeting stakeholder expectations despite a changing environmental context. Survivable systems are also insensitive to context changes. For example, a passively survivable system (AC) is able to maintain performance at or above minimal expectations. This is also the case for actively survivable systems, whether through adaptation (AD) or recovery (ADE).

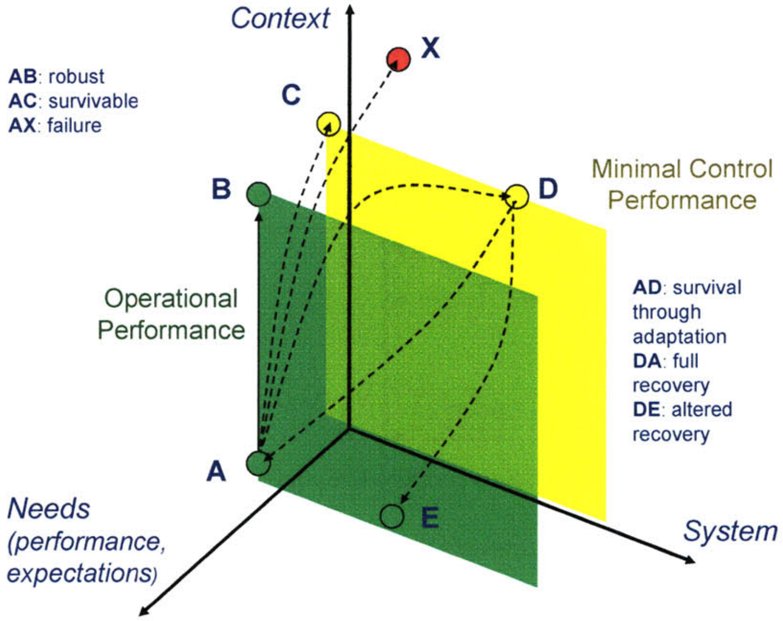


Figure 3-4. Sample Survivable and Robust System Trajectories within the "-ilities Space"

Although related, survivability and robustness are distinct. While designing for robustness focuses on accommodating permanent changes in context (*e.g.*, continuous noise factors, programmatic policy shifts), design for survivability focuses on the mitigating finite changes in context (*e.g.*, impulse event). Therefore, survivability can be considered a special case of robustness with a finite condition on disturbance duration. Figure 3-5 illustrates this distinction. Whereas the robust system might be able to accommodate three new epochs, the survivable system must only sustain utility [U] delivery during and after a finite disturbance *(e.g.*, the loss of U_2 in Epoch 2 followed by partial recovery of U_2 in Epoch 1b).

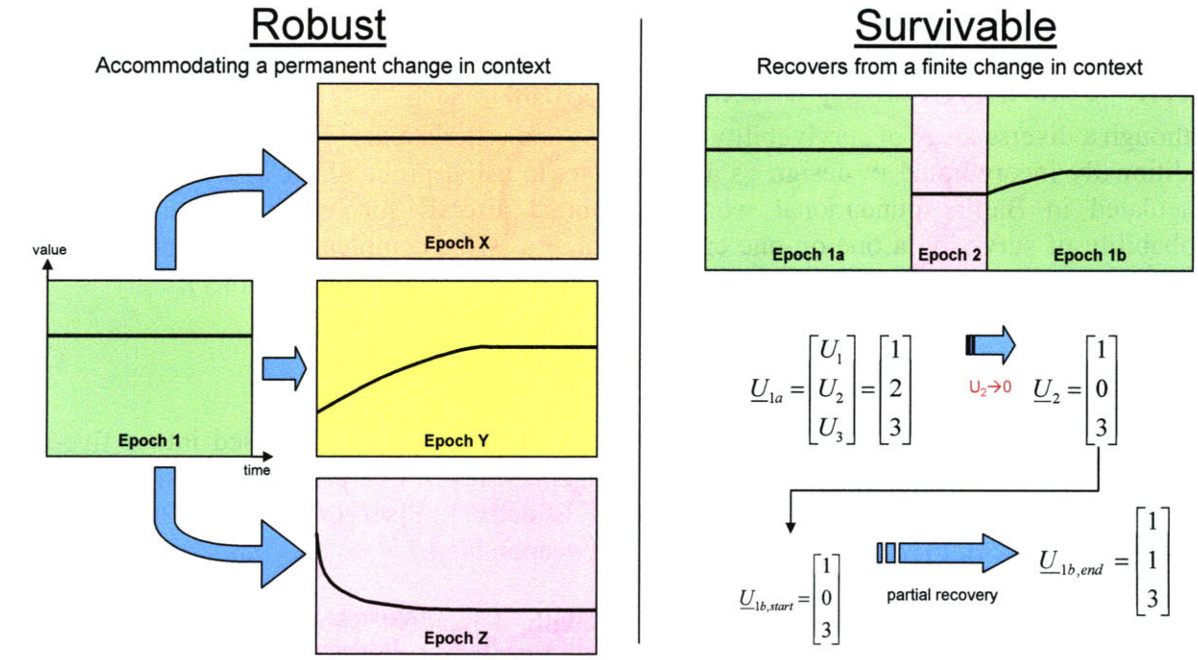

Robust
Accommodating a permanent change in context
value
time
Epoch 1
Epoch X
Epoch Y
Epoch Z
Survivable
Recovers from a finite change in context
Epoch 1a
Epoch 2
Epoch 1b
$\underline{U}_{1a} = \begin{bmatrix} U_1 \\ U_2 \\ U_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$
$U_2 \to 0$
$\underline{U}_2 = \begin{bmatrix} 1 \\ 0 \\ 3 \end{bmatrix}$
$\underline{U}_{1b,start} = \begin{bmatrix} 1 \\ 0 \\ 3 \end{bmatrix}$
partial recovery
$\underline{U}_{1b,end} = \begin{bmatrix} 1 \\ 1 \\ 3 \end{bmatrix}$

Figure 3-5. Distinguishing Between Survivability and Robustness

Given this distinction between survivability and robustness, one might ask *at what point do repeated disturbances constitute a change in context?* In other words, is there a clear demarcation between designing for survivability and designing robustness? As illustrated in Figure 3-6, there is no rigid division between the two "-ilities". Rather, there exists a continuum of disturbance encounters with survivability and robustness located on opposite ends of the scale. When the ratio of system life spent in nominal operating conditions (T_l) to the duration spent in disturbance epochs (T_d) is much less than one, then the focus is on design for survivability. However, in the limit that T_l approaches zero as intervals between disturbances become shorter, a new context has arisen and the focus in on design for robustness.

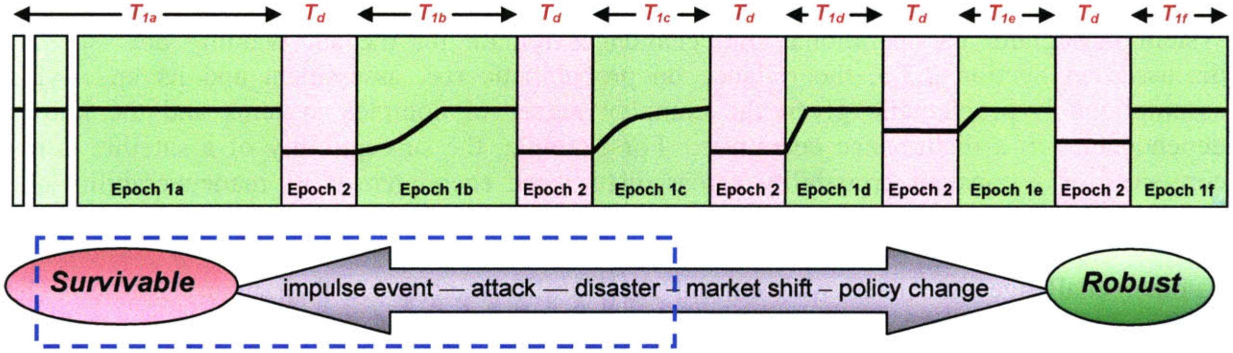


Figure 3-6. Continuum Between Survivability and Robustness

3.3. *Operationalizing Survivability*

3.3.1. Construct Validity of Existing Metrics

Although a diverse array of survivability definitions and criteria exist (Table 3-1), survivability is traditionally incorporated in design as a binary metric using probabilistic risk assessment. As articulated in Ball's foundational work on combat aircraft survivability (Ball 2003), the probability of surviving a one-on-one engagement, P_S, is the complement of the probability of hit, P_H (susceptibility), times the probability of kill given a hit, $P_{K|H}$ (vulnerability):

$$P_S = 1 - P_K = 1 - P_H \cdot P_{K/H} \tag{3-1}$$

(The susceptibility portion of the calculation, P_H, can be further decomposed into a five-step event tree or kill chain. For example, at the engagement level, five probability assignments are used to assess system susceptibility: P[weapon is active], P[sensor detects], P[fire control solution is obtained], P[weapon intercepts], and P[weapon hits].)

In order to reduce the complexity associated with dependent shot outcome probabilities, independent shot outcomes are assumed for computing survivability to multiple-shot engagements, $P_{S|E}$ (Ball 2003). For example, when the individual shots P_K are identical and equal to a single-shot probability of kill ($P_{K|SS}$) for all N shots, $P_{S|E}$, is:

$$P_{S|E} = 1 - P_{K|E} = (1 - P_{K|SS})^N \tag{3-2}$$

This logic is extended for computing, campaign-level survivability, *CS*, assuming a campaign of *N* missions with a constant mission survivability rate:

$$CS = (P_S)^N = (1 - P_K)^N \tag{3-3}$$

While these metrics for assessing single-shot, engagement, and campaign-level survivability provide an elegant mathematical framework for structuring and analyzing the survivability of a system throughout its operational life, challenges remain for the survivability analyst. As discussed in Section 2.3.3, the reliance on probabilistic risk assessment and its underlying assumptions is problematic given the complex nature of complex systems and the known dependencies in a disturbance encounter. For example, the susceptibility of a satellite is not conserved as a constant probability across disturbance encounters if its maneuverability and defensive countermeasures have been reduced by a previous encounter.

Another challenge associated with current survivability metrics are their binary nature. The ability of space systems to gracefully degrade to reduced levels of capability is frequently cited as an enabler of survivability (Hopkins 1971; Duren 2004; Siddiqi and De Weck 2006). However, a binary P_S value applied across systems during conceptual design does not internalize the magnitude or rate of system degradation—a capability which may be useful for distinguishing between systems that fail precipitously and systems that can achieve partially functional states. Additionally, for systems that are not safety-critical (*e.g.*, autonomous science missions), the impact of critical failures varies by when the failure occurs. To address the limitations of binary risk metrics, recent work (Wertz and Miller 2005; Wertz 2006) has extended traditional risk assessment techniques by introducing the concept of expected productivity. Expected productivity provides an aggregate measure of mission risk by quantifying mission performance based on the expected value of productivity (*e.g.*, number of images of star systems for observatories, number of rocks tested for sampling roving missions). While valuable for providing a continuous (non-binary) measure of the magnitude of risk, defining an aggregate productivity metric may be difficult or impossible for systems intended to accomplish multiple independent missions. The applicability of expected productivity may also be limited for non-scientific missions. In particular, the mission tasks of service-oriented space systems (*e.g.*, military satellites) may not necessarily be specified *a priori*, and critical survivability requirements may dictate the preservation of a minimal level of functionality over the entire mission duration.

The metrics discussed above generally view disturbances as sequences of short-duration variations in the operating environment. Another body of literature has framed this problem from a dynamic perspective focusing on both sustained variations in the environment and temporary shocks (Bogdanoff and Kozin 1985; Kharoufeh and Cox 2005). The shock-based reliability literature provides a time-dependent characterization of system state. However, the application of these shock models is focused on the part and component levels rather than system-level unit-of-analysis.

Another challenge for the system analyst relates to the architectural tradespace: how to conduct integrated tradeoffs regarding the varying cost, mission utility, availability, and survivability of alternative system designs? Because these characteristics are interdependent (as survivability design features and operational tactics may lower mission utility and increase cost), pursuing the highest survivability for a given design alternative does not necessarily maximize that system's mission effectiveness. For example, in the lead-up to World War II, 900 pounds of armor were added around the cockpit and fuel tanks of the Brewster F2A "Buffalo" fighter. While these modifications were based on combat data from the European theater, the higher wing loading decreased F2A's service ceiling, maneuverability, and maximum speed—turning a marginally acceptable fighter into an unacceptable one (Ball 2003).

To conduct tradeoffs among the availability, survivability, and capability of alternative designs, one approach (Ball 2003) is to define a measure of mission effectiveness, *MoME,* as a product of the three system attributes:

$$MoME = Availability \cdot Survivability \cdot Capability \tag{3-4}$$

MoME provides a single metric for evaluating the mission effectiveness of systems in an operational environment (informing strategic decisions such as managed attrition). However, the aggregated metric is of limited prescriptive value during design because the lifecycle costs of alternative designs are not constant. For example, a system with extremely high survivability that can be acquired at greater cost will have a higher *MoME* but may not allow a useful number of units to be purchased. Conversely, while a lower survivability rate for a satellite within a constellation may be more than offset by a higher availability or capability rate in the *MoME* computation, the implications of a lower survivability rate may be very negative from a constellation design perspective depending upon the satellite design life and replacement costs.

Other existing quantifications of survivability and related terms include the reliability function and inherent availability (Blanchard and Fabrycky 2006). The reliability function, also known as the survival function, provides the probability that a system will be operational for at least a given time, *t*.

$$R(t) = 1 - F(t) = e^{-t/MTBF} \tag{3-5}$$

Inherent availability, A_i, provides the probability that a system will be operational at any given time in the future, given a mean time between failure, *MTBF*, and mean time to repair, *MTTR*.

$$A_i = \frac{MTBF}{MTBF + MTTR} \tag{3-6}$$

In addition to providing only a binary metric for system health, the reliability function and inherent availability are of questionable construct validity for survivability. Both reliability and availability are concerned with the ability of a system to perform its function under prescribed environmental conditions whereas survivability is concerned with the state of a system that emerges based upon the interaction of that system with external disturbances. Furthermore, the assumed constant failure rates do not apply when disturbances are finite and impulsive in nature.

While existing survivability approaches have a remarkable legacy for improving the survivability of individual systems (*e.g.*, significantly enhanced combat aircraft survivability improvements from WWII to the present day), evaluation of survivability at higher levels in the system architecture (*e.g.*, constellation, space mission area) is both desirable and required given the increasing interdependencies among systems in networked environments. Based on the precepts discussed in the Section 3.2, three desirable criteria for evaluating survivability are: (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. In addition, it is also desirable to have survivability metrics that are intuitive as decision metrics and that don't require assumptions to be made regarding the independence of disturbance events. Guided by the definition of survivability in Section 3.2 and driven by these criteria, the following two sections introduce two metrics for the assessment of survivability in tradespace studies during conceptual design: (1) time-weighted average utility/utility loss and (2) threshold availability.

3.3.2. Survivability Metric #1: Time-Weighted Average Utility Loss

The development of metrics with construct validity for survivability as defined above requires evaluating a system's ability both to *minimize value losses* and to *meet critical value thresholds* before, during, and after environmental disturbances. There are many ways to operationalize value, and one approach is to use utility functions. In this thesis, a multi-attribute utility function is utilized (Keeney and Raiffa 1993) but the approach is not dependent on this formalization.[20] The multi-attribute utility function, $U(\underline{x})$, is an aggregation of single-attribute utility functions, $U^i(x^i)$, which reflect preferences over multiple single attributes, x^i (von Neumann and Morgenstern 1953). Given that attributes are varying over time, one can define $U(\underline{x}(t))$, or in shorthand, $U(t)$. Using this characterization of a system's utility delivery over the design life (T_{dl}), the time-weighted average utility may be defined:

$$\overline{U}_t = \frac{1}{T_{dl}} \cdot \int U(t)\ dt \tag{3-7}$$

In addition, time-weighted average utility loss may be defined 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:

$$\overline{U}_L = U_0 - \overline{U}_t \tag{3-8}$$

While time-weighted average utility loss is useful for evaluating the impact of various survivability features on a single system, it is less useful for comparisons across systems since U_o is not conserved across designs (*i.e.*, a constant utility loss applied across designs in the tradespace will have varying implications for survivability). For example, over-designed systems may have design utilities much greater than the utility threshold required in nominal conditions, $U_o >> U_x$, while U_o may approach U_x in systems with small performance margins. Therefore, to appreciate the survivability implications of a system's ability both to incorporate margin in value delivery and to minimize losses in value, it is necessary to evaluate time-weighted average utility loss relative to U_o.

3.3.3. Survivability Metric #2: Threshold Availability

As the expected (average) temporal utility experienced, time-weighted average utility assesses a system's lifecycle performance over nominal and disturbed environments. However, while this enables continuous evaluations to be made across systems regarding ability to minimize utility loss, it is a measure of central tendency that does not internalize ability to meet critical utility thresholds. Two threshold levels are identified on the emergency utility scale, $U(t)$. U_e is the minimally acceptable level in an emergency epoch and is therefore always zero. U_x is the level of utility provided by a design that achieves zero utility on the nominal scale when measured on the emergency scale.[21]

To evaluate the ability of a system to meet these critical utility thresholds, threshold availability, A_T, is proposed as a survivability metric. A_T is defined as the ratio of the time that $U(t)$ is above operable (required or emergency) utility thresholds (*i.e.*, time above thresholds [*TAT*]) to the total design life:

[20] 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 $V(t)$, the multi-attribute utility function, $U(t)$ (Keeney and Raiffa 1993), can be used to reflect the preference ordering of $V(t)$, if not the magnitude of that preference.

[21] While the definitions of the critical utility thresholds are complex, they are carefully chosen to reflect the preferences regarding design acceptability as elicited from the multi-attribute utility interview process.

$$A_T = \frac{TAT}{T_{dl}} \tag{3-9}$$

While structured similarly to the traditional metric of inherent availability (Blanchard and Fabrycky 2006), A_T is unique in that the critical utility threshold varies across nominal, disturbance, and recovery epochs. Performance losses, such as degradation or finite outage of capability, may be allowable in disturbance environments (*i.e.*, U_x and U_e both correspond to the minimally-acceptable level of utility delivery, $U(\underline{x})$=0, during their respective epochs).

The proposed metrics are related to existing frameworks and metrics in the literature. In general, the use of utility theory for survivability evaluation is discussed in Langworthy and Wells (1998). Threshold availability is essentially a modification of inherent availability that allows for a variable threshold of stakeholder expectations. Time-weighted average utility is analogous to the Quality-Adjusted Life Year (QALY). Often used in the medical community for patients evaluating treatment options, QALY is a multi-attribute quantity that varies as a function of time. QALYs scale the length of each year of remaining life by the quality of life expected in that year. The scaled years are then added to form QALYs. Thus, many years of low quality are equivalent to fewer years of high quality (Johannesson 1995).

3.3.4. Considerations for Implementation

One implication of value thresholds changing as a function of disturbance encounters is that definition and scale of a utility axis will vary across epochs and is therefore not consistent across the system lifecycle. For example, the set of attributes and their associated acceptability ranges, utility curves, and relative weights, may change for decision-makers across nominal and perturbed environmental states. This presents a challenge: how to present lifecycle utility data if the utility axis is a moving target? The general response to this challenge is to elicit the applicable multi-attribute utility functions across all potential epochs from the decision-maker. However, excessive resources may be required to collect such data without a process for bounding the large set of future environmental states.

If one assumes that the attribute set and weightings composing the utility function are constant throughout the mission, then one can define a utility function, $U(\underline{x})$, that reflects preference ordering across the normal, disturbance, and recovery epochs. $U(\underline{x})$ is constructed by increasing the acceptability range of the single-attribute utility functions, $U^i(x^i)$. First, the single- and multi-attribute utility functions during nominal operating conditions, $U_n(\underline{x})$, are elicited from the decision-maker. Second, the single- and multi-attribute utility functions during emergency conditions, $U(\underline{x})$, are elicited. Third, as described above, U_x and U_e are set to reflect the minimally acceptable level of utility during the nominal and disturbed periods, respectively (Figure 3-7). Given that $U(\underline{x})$ reflects decision-maker preference orderings across all epochs and provides a consistent scale, time-weighted average utility is computed using the emergency $U(\underline{x})$. This approach assumes that, during an emergency, decision-makers are willing to accept lower levels of performance but will raise expectations back to nominal levels following an emergency (*i.e.*, V_x>V_e).

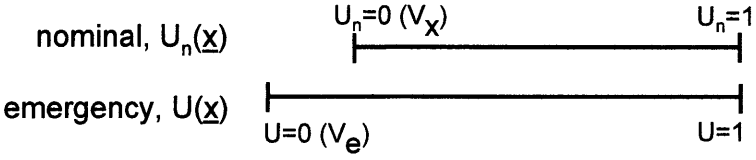


Figure 3-7. Setting Required and Emergency Value Thresholds

In summary, existing survivability metrics focus on assessing the physical integrity of systems using binary characterizations of system state. This chapter introduced the metrics of time-weighted average utility loss and threshold availability to capitalize on the benefits of evaluating survivability as a value-based, dynamic, and continuous system property. These metrics assess survivability based on the ability of systems to meet or exceed required levels of value delivery during nominal and perturbed environmental conditions. The metrics are unique but interdependent (*e.g.*, high average utility may imply high threshold availability, although high threshold availability may not imply high average utility). The metrics will be applied together in Chapter 5, Survivability Tradespace Experiments, to test their ability to discriminate among design alternatives.

4. Survivability Design Principles

This chapter addresses the second of the four research questions introduced in Section 1.3.2.

2. What design principles enable survivability?

The objective of this chapter is to develop and test a taxonomy of survivability design principles (*i.e.*, concept-neutral strategies of architectural choice) that may be used to enhance the generation of design alternatives during the critical front-end of product development (Figure 1-5). Existing sets of survivability design principles tend to exclude non-physical factors and to focus on concept-specific techniques. A general set of design principles allows the consideration of survivability strategies that may mitigate disturbances across the entire lifecycle of a given encounter. Within the context of tradespace exploration, the design principles are intended to augment the creativity of system designers by ensuring evaluation of a broad set of design alternatives.

Chapter 4 is composed of five sections. Following a brief survey of related survivability design principle frameworks (Section 4.1), survivability observations are made from historical systems to provide context (Section 4.2). The research approach for developing and testing the survivability design principles is then described and illustrated (Section 4.3). This section describes the process for enumerating the initial set of survivability design principles as well as the subsequent empirical testing to validate their completeness and rigor. Having established the validity of seventeen design principles, each principle (and its contribution to susceptibility reduction, vulnerability reduction, or resilience enhancement) is described (Section 4.4). The chapter concludes with a discussion of two different classes of survivability design principles, their temporal mapping to disturbance encounters, and implications for concept generation activities (Section 4.5).

4.1. Related Frameworks

A variety of taxonomies exist to inform the development of survivable systems. However, most of these taxonomies are domain-specific. For example, informed by the evolution of combat aircraft design, Air Force Instruction 62-201, "System Survivability," outlines eight strategies for achieving survivability: redundancy, threat-effect tolerance, active defense, deception, hardness, reconstitution, avoidance, and proliferation (SecAF 1994). Ball (2003) describes how these eight strategies may be incorporated into aircraft design through twelve survivability enhancement concepts. These twelve concepts are divided evenly between susceptibility reduction and vulnerability reduction concepts (Table 4-1).

Table 4-1. Twelve Survivability Enhancement Concepts (Ball 2003)

susceptibility reduction	**vulnerability reduction**
threat warning	component redundancy
noise jamming and deceiving	component location
signature reduction	passive damage suppression
expendables	active damage suppression
threat suppression	component shielding
weapons and tactics, flight performance, and crew training and proficiency	component elimination or replacement

Recognizing that large-scale information systems must mitigate elevated risks of intrusion and compromise, recent research has also focused on the design of survivable networks. Work at Carnegie Mellon's Software Engineering Institute discusses four properties system must exhibit in order to maintain service in the presence of attacks: attack resistance, attack recognition, recovery of full and essential services, and adaptation and evolution to mitigate future attacks (Ellison, Fisher et al. 1999). Table 4-2 shows their enumeration of strategies for achieving each property.

Table 4-2. Taxonomy of Strategies Related to Survivability (Ellison, Fisher et al. 1999)

Survivability Aspect	**Taxonomies of Strategies**
Resistance	• traditional security, including encryption and covert channels • diversity and maximized differences in individual nodes • analytic redundancy and voting • specialization, division of labor, trust, and information • continuous validation of trust • exhibited stochastic properties and random behavior
Recognition	• analytic redundancy and testing (including failures in software, encryption, and trust) • intrusion monitoring and suspicious activities • system behavior and integrity monitoring
Recovery	• physical and information redundancy • non-local copies of information resources • preparation, readiness, contingency planning, and response teams
Adaptation and Evolution	• general or specific changes to resist, recognize, or recover from new vulnerabilities that are discovered • broadcast of warnings to other nodes • broadcast of adaptation and evolution strategies • deterrence through retaliation or punishment

Other work focused on the design of survivable network services has applied lessons from biological and ecological systems. In particular, Nakano and Suda (2007) examine immune systems, social insects, and cellular systems as examples of biological networks that are inherently scalable, adaptable, and survivable. Immune systems provide protection by identifying and eliminating pathogens in a highly-distributed manner. Responses are highly adaptive and scalable and retain a memory of infections. Furthermore, the lack of centralized control eliminates the potential for a single-point-failure. Similarly, social insect colonies (*e.g.*, ants, wasps, termites, bees) achieve survivability as large-scale adaptive systems. Leveraging specialization (*e.g.*, foraging, nest-building, defense) and swarm intelligence, these colonies are survivable even if a large portion of the constituents are killed. Finally, cellular systems achieve survivability through communication mechanisms that enable systems to evolve from single cells in a highly decentralized and parallel process. Nakano and Suda (2007) extract five principles from these three examples of biological survivability: (1) emergence of collective behavior from simple behavior rules, (2) self-organization through localized interactions, (3) redundancy, (4) natural selection, and (5) diversity.

Another area of research related to the development of survivability design principles is the work of Jugulum and Frey (2007) to extract robust design strategies from the U.S. patent database. Jugulum and Frey define robustness in terms of product consistency; making the outputs of systems insensitive to variations in the environment, manufacturing, deterioration, and customer use patterns. As such, robust design focuses on the setting of design parameter and tolerance levels during detailed design activities. Noting that few robust design methods are directly applicable to the *generation* of concepts (in contrast to the many for *evaluation* of those concepts), Jugulum and Frey examined over 200 patents that claimed robustness as a key advantage over the prior art and proposed nineteen general robustness strategies which cross-cut domain applications (Figure 4-1).

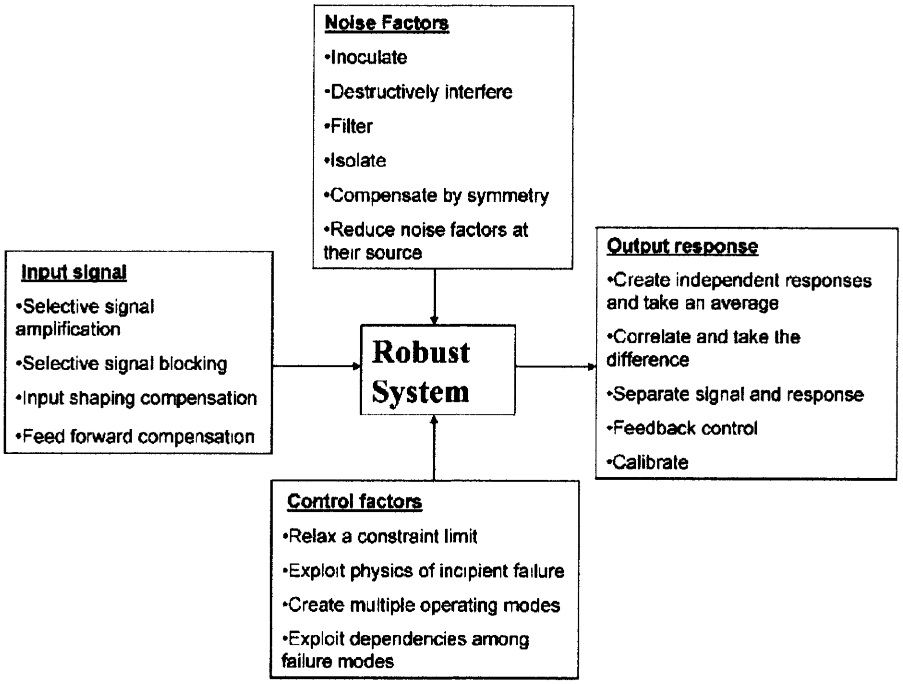

Noise Factors
•Inoculate
•Destructively interfere
•Filter
•Isolate
•Compensate by symmetry
•Reduce noise factors at their source
Input signal
•Selective signal amplification
•Selective signal blocking
•Input shaping compensation
•Feed forward compensation
Robust System
Output response
•Create independent responses and take an average
•Correlate and take the difference
•Separate signal and response
•Feedback control
•Calibrate
Control factors
•Relax a constraint limit
•Exploit physics of incipient failure
•Create multiple operating modes
•Exploit dependencies among failure modes

Figure 4-1. Representation of Robust Design Strategies in a P-Diagram (Jugulum and Frey 2007)

Given that survivability is a subset of robustness (Section 3.2.3), many robustness strategies are synergistic with survivability design principles. However, it is important to note two distinguishing characteristics. First, the unit of analysis and scope of traditional robust design techniques is frequently smaller and more detailed than the system-level survivability examined in this thesis. Second, threats to robustness typically consist of continuous, statistically-sampled noise with limited magnitude. This stands in contrast to survivability where finite-duration disturbances originate from sources external to the product system.

The survivability design principles derived in this chapter are complementary to existing taxonomies given their general nature and architectural scope. In contrast to the domain-specific survivability frameworks for combat aircraft and network design, the design principles introduced here are intended for general applicability. The design principles are distinguished from the enumeration of robust design strategies by considering a larger unit of analysis (*i.e.*, system architectures rather than component technologies) and by focusing on the mitigation of system-external disturbances of finite duration rather than the design of systems insensitive to continuous noise factors. This latter contrast is representative of the overall distinction between survivability and robustness: survivability is a special case of robustness with a finite condition on disturbance duration (Section 3.2.3).

4.2. Survivability Observations from Historical Systems

Before making prescriptive statements regarding survivability design principles, it is necessary to understand how designers have previously pursued system survivability. While Section 2.1 provided an overview of current approaches to designing for survivability, it is also helpful to examine the survivability strategies of deployed systems. In this section, a retrospective overview of two systems is provided: the B-17 Flying Fortress in World War Two (WWII) and the U.S. Nuclear Command and Control System (NCCS) during the Cold War. In both cases, survivability was key driver in the system design and operation.

4.2.1. B-17 Flying Fortress

Ball (2003) provides an excellent history of the B-17 Flying Fortress, a U.S. Army Air Corps bomber that evolved into its classic design over the course of several modifications to enhance survivability. As discussed in Ball, the B-17 is one of the most famous bombers of WWII. Over 12,000 were built between July 1940 and August 1945, and B17's carried 40% of the bombs dropped in the European theater. The B-17's were first deployed by the British in groups of three to four in daylight raids over France, Germany, and Norway. Their initial survivability was very poor as the B-17C was lacking in firepower and highly susceptible to concentrated fighter attacks. In fact, the German Luftwaffe referred to the B-17 as the "Flying Coffin". However, operational experience with the B-17 influenced the development of new mission tactics and several design evolutions to enhance survivability. In response to the threat posed by German fighters, the commanders began deploying the B-17 in formations consisting of hundreds of bombers. While this increased the probability of early detection, the tactic enabled mutual protection by concentrating defensive firepower. Eight major design modifications were also made to enhance survivability. These modifications included the addition of heavy armor plating, self-sealing fuel tanks, and equipment to support as many as thirteen heavy machine guns.

The evolutionary approach taken to enhance B-17 survivability—incorporating feedback from combat experiences in successive design iterations—stands in contrast to current approaches to survivability. With the developments of stealth, precision targeting, and stand-off weapons, combat aircraft survivability has improved by orders of magnitude. However, sensitivity to downside losses has increased as the absolute number of airborne platforms is reduced (*e.g.*, contrast the 12,000 B-17's to the 21 B-2's built). These sensitivities to even very low losses (*e.g.*, F-117 shoot-down in Kosovo) coupled with the limited opportunities for experiential learning in combat underscore the importance of survivability for all design iterations. However, the focus on platform survivability raises the question of whether the architectural survivability (*i.e.*, overall survivability of the mission capability) has been sacrificed due to the tremendous reduction in the number of units purchased.

4.2.2. U.S. Nuclear Command and Control System

The collection of offensive, defensive, and intelligence systems operated by U.S. Strategic Command to fulfill the mission of strategic deterrence is perhaps the most notable effort to develop a survivable system architecture. Military systems for nuclear war may be broadly decomposed into reconnaissance systems for target selection; ground- and space-based sensors for early warning; fixed and mobile command and control centers; and the triad of offensive submarines, bombers, and land-based intercontinental ballistic missiles. Given that the systems were designed to operate in a wide range of extremely hostile environments—from the extreme blast, heat, and fallout of a nuclear exchange to the impact of a chemical, biological, or electromagnetic pulse (EMP) weapons—a host of survivability lessons may be extracted from the design of their technical, operational, and organizational architecture.

Rather than analyzing all military systems associated with strategic deterrence, the focus here is on the U.S. nuclear command and control system (NCCS) during the Cold War. When the U.S. switched from a policy of massive retaliation to one of flexible response in 1961, survivable communications (*i.e.*, maintaining operational capability after a Soviet first-strike) between central authorities and the nuclear forces became a military requirement.[22] As a system designed against this nuclear decapitation attack scenario, the NCCS is a strong candidate for a case study on survivability.

The NCCS may be functionally decomposed into five areas: situation monitoring, tactical warning, decision-making, force management, and force direction (Critchlow 2006). Situation monitoring includes both the collection of strategic intelligence to anticipate crises and weather monitoring to support airborne operations. Tactical warning consists of the set of activities to determine the origin, size, and target of an attack. In supporting decision-makers in crafting a response, tactical warning requires a high degree of certainty (*e.g.*, dual phenomenology provided by satellites and radars). Force management and direction includes the standard operating procedures involved in assuring negative and positive control (*i.e.*, prevention of accidental launches and implementation of presidential release orders, respectively).

The current survivability of the NCCS is attributed to four design principles: (1) hardening, (2) mobility, (3) redundancy, and (4) concealment (Critchlow 2006). These four design principles manifest themselves differently in the various nodes and links of the NCCS (*e.g.*, contrast hardening of the NORAD Cheyenne Mountain Complex to the Milstar satellite constellation). Additionally, each design principle does not contribute equally to architecture survivability. For example, in the early 1980's, there were concerns that Soviet strategic forces could overwhelm virtually all U.S. ground-based command and control and that the U.S. was dependent on airborne command posts and TACAMO relay aircraft for post-attack control over the submarine force (Bracken 1983; Blair 1985). These concerns suggest that mobility was more important for achieving NCCS survivability than the hardening and redundancy provided by the network of fixed command locations in the Pentagon, Offutt Air Force Base, Fort Ritchie, and Cheyenne Mountain (Critchlow 2006).

[22] If early warning sensors detected a nuclear attack by the Soviet Union during the period of 1955-60, U.S. policy was to launch a full retaliation between the time of launch and strike. As such, the NCCS was superfluous after the Presidential release order and was therefore not originally designed for survivability (Bracken 1983).

While the four design principles of NCCS survivability discussed previously provide a fairly complete enumeration of physical strategies for achieving survivability, the discussion neglects critical architectural elements of operational behavior and organizational design. For example, with decision cycles in a nuclear war measured in minutes (Blair 1985), development of a scripted operational plan for every conceivable contingency may be as essential to providing a credible deterrent against a decapitation threat as the survivability of the nuclear force itself.

The sensitivity of NCCS survivability to operational behavior and organizational design is best illustrated in the transition in the 1960's away from the massive retaliation policy to a flexible response paradigm that required NCCS survivability (Bracken 1983). Facing the challenge of inheriting a legacy NCCS infrastructure that was not designed for survivability but without resources to build a new infrastructure, designers succeeded in re-architecting the existing NCCS infrastructure for survivability by restructuring tactics, procedures, and operating rules. In particular, the decapitation risk was mitigated by making the presidential command center a "safety catch" that, when operational, prevented other command centers from firing. If the safety catch was removed, second-strike emergency authorization was implicitly granted to decentralized authorities (*i.e.*, one- and two-star generals), removing the prospect of a single-point failure in the command structure.

Four main lessons may be extracted from tracing the evolution of NCCS through the Cold War with implications for survivability design principles. First, the success in re-architecting the system for survivability in the 1960's illustrates the importance of considering methods that extend beyond the domain of physical design to include organizations and operational behavior. Given the success in transitioning the NCCS in the 1960's from a non-survivable to a survivable system without major physical modifications, might it be possible similarly to transition existing systems to less vulnerable states today by restructuring procedures and operating rules? Second, the emphasis on executing scripted contingency plans underscores the criticality of timely decision-making under uncertainty within hostile environments. Third, the strategic interactions characterizing the NCCS context (*e.g.*, Mutually Assured Destruction) suggests that it is not adequate to consider individual disturbance events when dealing with an intelligent adversary. Rather, it is necessary to take a longer view by considering design principles for survivability which may influence the behavior of adversaries over multiple encounters. Fourth, while the NCCS is an excellent case for enumerating design principles for survivability, it is important to note its limitations: (1) the design principles explicitly linked to NCCS survivability (Critchlow 2006) are limited to the physical domain, and (2) the design principles as manifested in the NCCS are unlikely to be affordable solutions to current survivability challenges. While addressing the latter issue of incorporating cost-benefit trade-offs for survivability features in the analysis is the subject of Chapters 5, 6, and 7, the present chapter focuses on an approach for expanding the number of survivability design principles under consideration.

4.3. Approach: Generating and Evaluating Design Principles

A four-step approach is pursued for generating and evaluating the survivability design principles: (1) deduce design principles from generic system-disturbance representation, (2) select operational systems with survivability requirements, (3) trace survivability enhancement features on operational systems to design principles, and (4) revise design principle set to reflect empirical observation.

Evaluating the design principles through empirical testing is a critical aspect for validation. In addition to objectivity and control, empiricism—the doctrine that knowledge derives from experience—comprises an underlying principle of the scientific method. The benefits of empiricism for enriching the quality of systems engineering research and for enhancing the standing of systems engineering in the academic community have been well documented (Valerdi and Davidz 2007). In the process of defining survivability design principles, empirical testing ensures completeness, logical consistency, and taxonomic precision. Testing for both internal and external validity is an essential step in the development of a verifiable, repeatable, and theoretically-sound methodology (Frey and Dym 2006).[23]

4.3.1. Deductively Enumerate Design Principles

The first step of enumerating survivability design principles is based on a generic system-disturbance framework. Having established a definition of survivability (Chapter 3) and reflected on survivability observations from existing frameworks (Section 4.1) and historical systems (Section 4.2), a preliminary framework was developed for visualizing and deriving design principles of survivability. Consisting of the minimum set of elements needed to describe the interaction between a system and a given hostile environment, Figure 4-2 illustrates a simple network representation of heterogeneous nodes and arcs of the technical system architecture, a system operator characterized by an internal change agent, and a hostile environment characterized by an external change agent. Changes in the arrangement of these elements are used to provide insights into various survivability strategies.

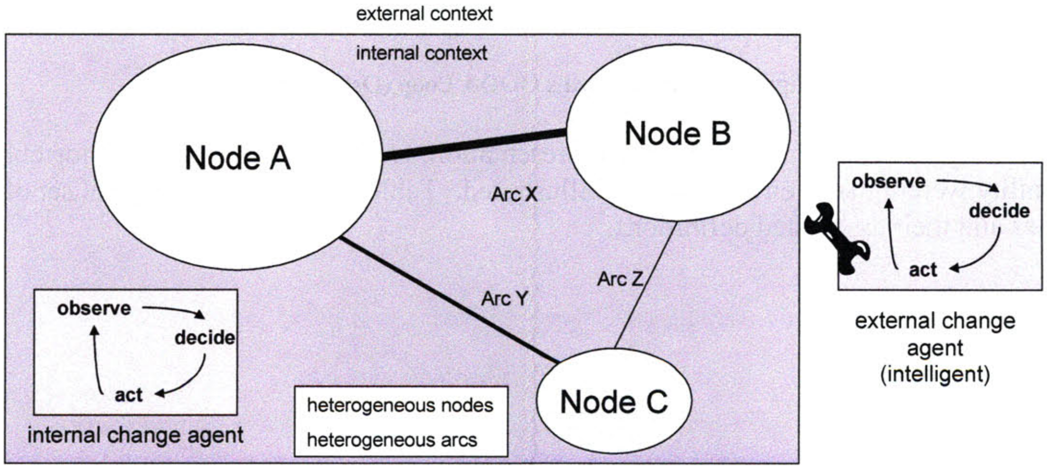


Figure 4-2. Generic System-Disturbance Representation

The external change agent in Figure 4-2 is an abstraction of a source of disturbances, which could consist of an intelligent adversary or natural phenomenon. For the case of an intelligent adversary, decision-making of the external change agent is based on an "observe → decide → act" (ODA) cycle. Observation of the system and its environmental context informs value-

[23] While internal validity is concerned with logical consistency, external validity refers to the empirical relevance of the theory (*e.g.*, Can the findings be generalized? Is the methodology applicable outside of a laboratory-setting?) (Neuman 2006).

maximizing decision-making, which in turn governs disturbance activity. This model of the behavior of the external agent is inspired by the Boyd cycle, also known as the Observe, Orient, Decide, and Act (OODA) loop (Osinga 2006). (In this research, the *orient* phase is considered a subset of the *decide* phase.) Figure 4-3 provides an illustration of the dependencies among the four processes of the OODA loop. Developed to prescribe activity in combat, the OODA loop emphasizes getting "inside" the decision cycle of an enemy to enhance military success and survivability. The ODA loop representation of the decision-making of an intelligent adversary was employed to parse out the design principles of survivability that are related to the strategic interaction between the internal and external change agents.

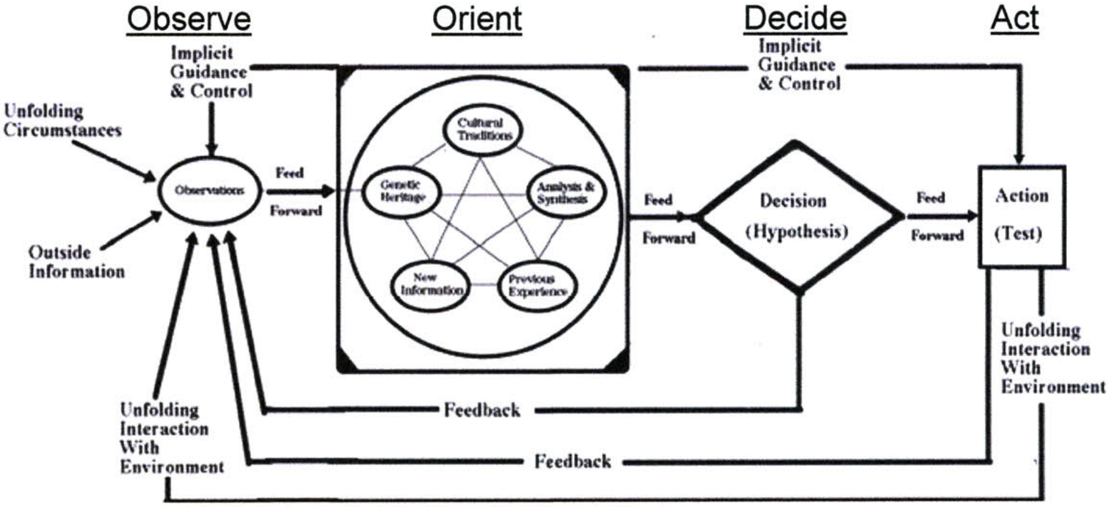


Figure 4-3. John Boyd's OODA Loop (Osinga 2006)

Utilizing the generic system-disturbance representation, twelve design principles for enhancing survivability were initially enumerated and illustrated. Table 4-3 shows the original set of design principles and their associated definitions.

Table 4-3. Initial Set of Twelve 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 disturbance
Type II Survivability (Reduce Vulnerability)		
2.1	**hardness**	resistance of a system to deformation
2.2	**evolution**	alteration of system elements to reduce disturbance effectiveness
2.3	**redundancy**	duplication of critical system components to increase reliability
2.4	**diversity**	variation in system elements (characteristic or spatial) to decrease effectiveness of homogeneous disturbances
Type III Survivability (Increase Resilience)		
3.1	**replacement**	substitution of system elements to improve value delivery
3.2	**repair**	restoration of system to improve value delivery

As an example of how each design principle was illustrated, the Type I design principle of concealment was abstractly represented as a blending of the system nodes and links into the internal context whereas the Type II design principle of hardness was represented as an increase in the thickness of the shells around each node. Richards et al. (2007) provides a complete description of the initial twelve design principles.

4.3.2. Select Existing Survivable Systems

Having deductively enumerated twelve survivability design principles from an abstract framework, the design principles were empirically tested against operational systems with critical survivability requirements. In selecting systems for examination, four factors were considered: (1) stratified sampling across the aerospace domain, (2) the disturbance environments associated with a system's operational context, (3) access to data regarding system survivability features, and (4) a desire to extract insights from systems that achieve survivability at multiple levels in their system architectures. Given these factors, the A-10A Warthog combat aircraft, UH-60A Blackhawk helicopter, F-16C combat aircraft, and Iridium satellite communications network were selected for the empirical tests. This sample draws across four major classes of aerospace systems: helicopters designed for low-vulnerability, aircraft designed for low-susceptibility, aircraft designed for low-vulnerability, and a resilient satellite constellation. The survivability features of these systems address both natural and hostile environmental disturbances. Given the maturity of all four systems, a large amount of open-source data is available regarding their survivability features and operational experience. Finally, in contrast to the three military aircraft systems, the selection of Iridium enables analysis of survivability at a higher level in the system architecture—where survivability is achieved through generalized dependence (Neumann 2000) among a constellation of satellite systems rather individual constituent nodes.

To illustrate the testing of the preliminary set of design principles, the UH-60A Blackhawk helicopter will be used as a running example in the following two sections. (The empirical testing of design principles against the survivability enhancement features of the A-10A, F-16C, and Iridium network is described in Appendix A, Appendix B, and Appendix C, respectively.) In selecting the Blackhawk, the unit of analysis is a piloted helicopter operating in a hostile combat environment (*e.g.*, confronting guns and missiles carried by enemy air and ground systems). The required value threshold for the system is a safe and successful completion of a given mission. The emergency value threshold is met if the crew and vehicle are able to exit the combat zone despite a failure to achieve mission objectives. Survivability features may add value over the entire lifecycle of a given disturbance (*e.g.*, Epoch 1a, Epoch 2 and Epoch 1b).

4.3.3. Trace Survivability Features to Design Principles

The process of empirically testing the initial survivability design principles begins by attempting to establish traceability from survivability features in operational systems to the baseline set of design principles (*e.g.*, a bumper shield installed on a satellite for mitigating the impact of orbital debris would map to the design principle *hardness*). These mappings are not necessarily one-to-one. For example, weapon systems on a combat aircraft might be used for *prevention*, *deterrence*, and *preemption*—each of which constitutes a unique design principle of Type I survivability. By conducting such mappings for the survivability features over multiple systems, the validity of the design principles can be evaluated (*i.e.*, Are there survivability features that cannot be traced to any design principles? Does each design principle have a clear meaning within the domain of a particular class of systems?).

In establishing traceability, matrices are used to qualitatively illustrate the mapping of survivability features in operational systems to the twelve design principles. One matrix is constructed for each system under investigation. Survivability features (grouped by subsystem) comprise the rows and the baseline set design principles comprise the columns. Relationships are represented with "X" marks – an indication that one of the functional requirements of the feature (row) achieves survivability utilizing a particular set of design principles (columns). It is expected that utilization of a particular feature should involve the application of one or more design principles. If logical inconsistencies or other issues arose while establishing traceability, those portions of the matrices are shaded in grey. These grey regions are subjected to more rigorous analysis and will potentially inform improvements to the existing design principle set.

The, UH-60A Blackhawk, a medium-lift utility or assault helicopter used by the U.S. Army and over twenty military services around the globe, provides a representative example of the process of tracing the survivability features in existing systems to the survivability design principles. As a tactical transport, the UH-60A lift capability can accommodate a fully-equipped eleven-person infantry squad or a 105 mm Howitzer, its crew of six, and 30 rounds of ammunition (USA 2006). Just as the A-10 Warthog design was inspired by the need to address the vulnerabilities of the Air Force's fixed-wing aircraft in Vietnam (Appendix A), development of the UH-60A was a direct response to the large number of Army helicopters lost in Southeast Asia between 1963 and 1973. Selected as the winner of the Utility Tactical Transport Aircraft System competition, the UH-60A had a firm design requirement on vulnerability. Figure 4-4 illustrates some of its vulnerability reduction features, including redundant or armored components and systems, a structure tolerant to 23mm shells and designed to progressively crush in the event of a crash, and passive stabilization strategies in the event of a loss of rotor control (Ball 2003).

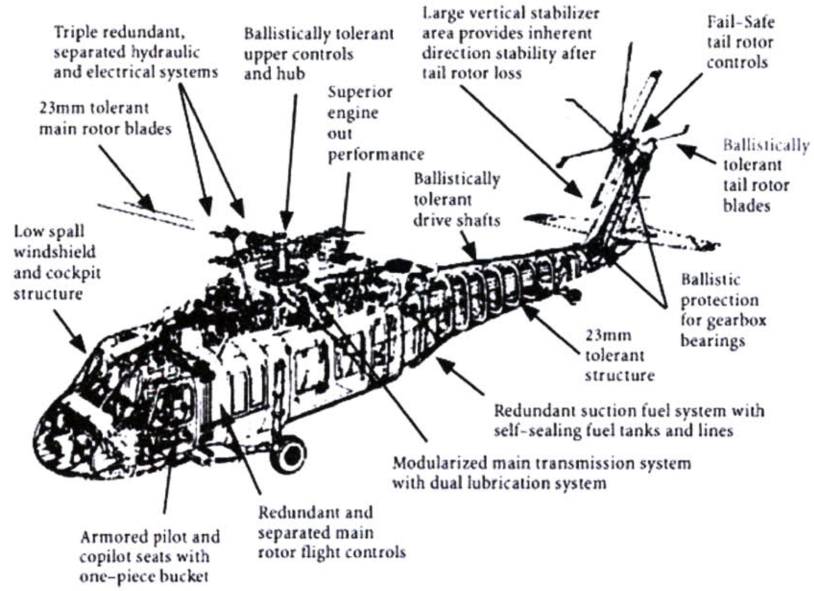

Triple redundant, separated hydraulic and electrical systems
Ballistically tolerant upper controls and hub
Large vertical stabilizer area provides inherent direction stability after tail rotor loss
Fail-Safe tail rotor controls
23mm tolerant main rotor blades
Superior engine out performance
Ballistically tolerant tail rotor blades
Ballistically tolerant drive shafts
Low spall windshield and cockpit structure
Ballistic protection for gearbox bearings
23mm tolerant structure
Redundant suction fuel system with self-sealing fuel tanks and lines
Modularized main transmission system with dual lubrication system
Redundant and separated main rotor flight controls
Armored pilot and copilot seats with one-piece bucket

Figure 4-4. Some Vulnerability Reduction Features on the UH-60 Blackhawk (Ball 2003)

First introduced into the U.S. Army in 1979, Blackhawk helicopters have served in combat, from the 1983 Grenada invasion to the present day in Iraq. As noted in (Ball and Atkinson 1995), the emphasis on reducing the UH-60A vulnerability paid off in Grenada where the Blackhawk "sustained and survived small arms and 23mm anti-aircraft fire while carrying out its mission of transporting and supporting Army Rangers. Of the 32 Blackhawks used in Grenada, ten were damaged in combat. One helicopter had 45 bullet holes that damaged the rotor blades, fuel tanks, and control systems, yet it still managed to complete its mission."

Table 4-4. Tracing of UH-60A Blackhawk Survivability Features to Initial Design Principles

		Design Principles											
		Type I						Type II				Type III	
	UH-60A: Sample Survivability Features	prevention	mobility	concealment	deterrence	preemption	avoidance	hardness	evolution	redundancy	diversity	replacement	repair
rotor blade and drive train	modularized transmission (eliminates exposed shaft and lube system)												
	operates 1+ hours after loss of all oil							X		X			
	noncatastrophic failure allows autorotation												
	rotor blades tolerant to high-explosive incendiary (HEI) projectile							X					
	elastomeric hub with no lube, tolerant to HEI projectiles							X					
	large vertical tail with long boom provides anti-torque in forward flight												
	shaft supports provide damping for damaged shaft							X					
	no bearings or lube in cross-beam rotor												
	tail rotor blades ballistically tolerant							X					
	damaged parts of tail rotor thrown away from helicopter												
structure	crashworthy armored seats and retention system							X					
	shatterproof cockpit window							X					
	minimum-spall materials used in cockpit							X					
	kevlar armor to stop HEI fragments							X					
	airframe progressively crushes on impact							X					
	protective armor withstands hits from 23mm shells							X					
fuel system	two self-sealing/crashworthy tanks located away from ignition sources									X	X		X
	short, self-sealing feed lines												X
	engine-mounted suction pumps												X
	cross feed capability									X			
	closed cell foam around tanks							X					
	hydrodynamic tolerant fuel tanks							X					
propulsion	maneuverability		X				X						
	two widely separated engines										X		
	titanium fire walls							X					
	fire detection with two shot fire extinguishing												X
	widely separated engine to transmission input modules										X		
	no fuel ingestion							X					
	good one engine out capability									X			
flight control	two independent, separated mechanical controls with disconnects									X	X		
	tail rotor is stable if pitch rod is severed												
	spring drives tail rotor blades to fixed pitch setting if control signal lost												
	controls are ballistically tolerant							X					
	two independent, separated, and shielded hydraulic power subsystems									X	X		
	third electrically driven backup power subsystem									X	X		
	quick disconnects and leak isolation valves												
	less flammable hydraulic fuel							X					
armament	two door-mounted 7.62mm machine guns	X			X	X							
	infrared jamming flares			X									
	chaff dispenser			X									
	missiles and rockets	X			X	X							

Table 4-4 presents the results of tracing UH-60A survivability features to the design principles. With a clear emphasis on vulnerability reduction (Type II survivability), 41 survivability features were identified (Ball and Atkinson 1995; USA 2006) and divided into six areas: rotor blade and drive train, structure, fuel system, propulsion, flight control, and armament. Many insights were revealed while mapping the 41 features to the design principles. Most critically, eight of the UH-60A survivability features were found to be untraceable to the original set of twelve design principles. Three potentially new design principles are discussed to account for these discrepancies. In addition, needed revisions were found to two existing design principles.

The first row of Table 4-4, "modularized transmission eliminates exposed high speed shafts and multiple lube systems with exposed oil components," is the first UH-60A survivability feature that does not employ any of the existing design principles. As a survivability design which reduces vulnerability to a "loss of lubrication" kill mode (Ball and Atkinson 1995), this feature employs a hazard elimination strategy. Hazard elimination, a reduction in the number of system failure modes, is a foundational goal of system safety (and followed by hazard reduction, hazard control, and damage reduction in priority in system safety engineering) (Leveson 1995). However, hazard elimination is not represented in the preliminary set of design principles. This gap is also apparent for the survivability feature of "no cross bearings or lube" in the cross-beam tail rotor drive system. A similar problem is also evident for the survivability feature of [fuel system] short, self-sealing fuel lines. While the ability of the fuel lines to self-seal (and hence reduce the probability of fuel supply depletion kill mode) is recognized as employing the design principle of *repair*, the shortness of the lines—reducing susceptibility to fires and explosions—is not traced to any of the design principles. Integrating across these three examples, the first unique insight from the UH-60A is a need for a design principle of *failure mode reduction.*

The second new design principle derived from the UH-60A stems from five untraceable survivability features: [rotor blade and drive train] (1) non-catastrophic failure allows autorotation (*i.e.*, forward momentum of helicopter provides some lift by spinning main rotor in the event engine failure), (2) large vertical tail with long boom provides anti-torque in forward flight (*i.e.*, forward momentum provides some yaw control if tail rotor is lost), (3) damaged parts of tail rotor thrown away from helicopter, [flight control] (4) tail rotor is stable if pitch rod is severed, and (5) spring drives tail rotor blades to fixed pitch setting if control signal lost. Each of these survivability features leverage "the physics of the incipient failure" to prevent or delay the failure mode (Clausing and Frey 2005). From a functional perspective, the underlying principle employed by each of these five survivability features is an elimination of immediate danger by automatically compensating for failure (*i.e.*, a *fail-safe* design).

Two problematic UH-60A feature mappings inform the third new design principle: the need for *containment* within Type II survivability. By incorporating the feature of [flight control] quick disconnects and leak isolation valves, the Blackhawk reduces the probability of a hydraulic fluid fire by containing the propagation of failure (Ball and Atkinson 1995). This containment principle, which fits within the system safety technique of hazard control, is also employed by the incorporation of shaft supports that provide damping of a damaged shaft [rotor blade and drive train] to protect the overall structural integrity. As with many systems with high-energy transfers, helicopters are tightly-coupled and highly-tuned systems (*i.e.*, they exhibit impedance matching) in order to maximize efficiency. A vulnerability of such systems is the tendency for failures to rapidly propagate. The UH-60A clearly incorporates the principle of containment to limit the propagation of such failures.

In addition to the three design principles uncovered above, the Blackhawk test case also exposed problematic aspects of two of the original survivability design principles: (1) the need to decompose the design principle of diversity into *heterogeneity* and *distribution* and (2) the need to distinguish between *redundancy* and *margin.* As defined in the preliminary design principle set, diversity is characteristic or spatial variation to limit the effectiveness of homogeneous disturbances. This is an extremely broad definition that includes variation in both the properties (*i.e.*, heterogeneity) and locations of system elements (*i.e.*, distribution). These are two fundamentally different concepts. Five UH-60A examples of the diversity design principle that would be clearly mapped to a distribution principle include the survivability features of [fuel system] two self-sealing/crashworthy tanks located away from ignition sources, [propulsion] two widely separated engines, widely separated engine to transmission input modules, [flight control] two independent, separated mechanical controls with disconnects, and two independent, separated, and shielded hydraulic power subsystems.

Redundancy, which was originally defined in terms of duplication of critical system components, is a poor fit for two survivability features in the Blackhawk: [rotor blade and drive train] operates 1+ hours after loss of all oil and [propulsion] good one engine out capability. Redundancy implies substitution of components to maintain a consistent level of performance whereas an ability to fly for over an hour after loss of oil is indicative of design *margin.* While redundancy and margin are related in terms of having something "extra," they are fundamentally different concepts because margin implies a continuum of capability which, if reduced, may impact end-user value.

4.3.4. Revise Design Principles

The final step of generating and evaluating a general set of survivability design principles is to revise the framework following each empirical test. In this iterative process, there is an inherent tension among competing desires for clarity, mutual independence, collective exhaustiveness, and maintaining a tractable number of principles. For example, the process of attempting to trace the survivability features of the UH-60A Blackhawk helicopter to the existing design principles was a strong driver against minimizing the size of the set. Not all of the survivability features of the UH-60A were successfully mapped to the existing design principles as the size of the set of Type II design principles was expanded by five.

Table 4-5. Revisions to Design Principles from UH-60A Empirical Test

	Insight	Implication
1	Survivability features that employ design margin are untraced	Add new Type II design principle of margin
2	Imprecise definition of diversity – includes both characteristic and spatial	Decompose diversity into heterogeneity and distribution
3	Survivability features that reduce the number of system failure modes are untraced	Add new Type II design principle of failure mode reduction
4	Survivability features employing "physics-of-failure" are untraced	Add new Type II design principle of fail-safe
5	Survivability features that limit or slow the propagation of failures are untraced	Add new Type II design principle of containment

As shown in Table 4-5, extensive modifications were required of the Type II survivability set to accommodate the results of the UH-60A empirical test: the decomposition of diversity into the design principles heterogeneity and distribution; the distinction drawn between redundancy and margin; and the addition of the design principles of failure mode reduction (2.6), fail-safe (2.7), and containment (2.9). While heterogeneity, distribution, and margin are specializations of the original set of design principles, failure mode reduction, fail-safe, and containment are fundamentally new design principles which were excluded from the preliminary framework. These modifications are valuable for helping systems engineers consider a larger set of survivability techniques. Additionally, capturing the subtle functional differences among design principles may expand the design space enumerated from form-function mapping in conceptual design. Table 4-6 shows the tracing of the Blackhawk survivability features to the revised set of design principles.

Table 4-6. Tracing of UH-60A Blackhawk Survivability Features to Revised Design Principles

		Design Principles																
		Type I (Reduce Susceptibility)						Type II (Reduce Vulnerability)									Type III	
	UH-60A: Sample Survivability Features	prevention	mobility	concealment	deterrence	preemption	avoidance	hardness	redundancy	margin	heterogeneity	distribution	reduction	fail-safe	evolution	containment	replacement	repair
rotor blade and drive train	modularized transmission (eliminates exposed shaft and lube system)												X					
	operates 1+ hours after loss of all oil							X		X								
	noncatastrophic failure allows autorotation													X				
	rotor blades tolerant to high-explosive incendiary (HEI) projectile							X										
	elastomeric hub with no lube, tolerant to HEI projectiles							X										
	large vertical tail with long boom provides anti-torque in forward flight													X				
	shaft supports provide damping for damaged shaft															X		
	no bearings or lube in cross-beam rotor												X					
	tail rotor blades ballistically tolerant							X										
	damaged parts of tail rotor thrown away from helicopter													X				
structure	crashworthy armored seats and retention system							X										
	shatterproof cockpit window							X										
	minimum-spall materials used in cockpit							X										
	kevlar armor to stop HEI fragments							X										
	airframe progressively crushes on impact							X										
	protective armor withstands hits from 23mm shells							X										
fuel system	two self-sealing/crashworthy tanks located away from ignition sources								X	X		X						X
	short, self-sealing feed lines												X					X
	engine-mounted suction pumps																	X
	cross feed capability								X	X								
	closed cell foam around tanks							X										
	hydrodynamic tolerant fuel tanks							X										
propulsion	maneuverability		X				X											
	two widely separated engines											X						
	titanium fire walls							X										
	fire detection with two shot fire extinguishing																	X
	widely separated engine to transmission input modules											X						
	no fuel ingestion							X										
	good one engine out capability									X								
flight control	two independent, separated mechanical controls with disconnects								X	X		X						
	tail rotor is stable if pitch rod is severed													X				
	spring drives tail rotor blades to fixed pitch setting if control signal lost													X				
	controls are ballistically tolerant							X										
	two independent, separated, and shielded hydraulic power subsystems								X	X		X						
	third electrically driven backup power subsystem								X	X	X	X						
	quick disconnects and leak isolation valves															X		
	less flammable hydraulic fuel							X										
armament	two door-mounted 7 62mm machine guns	X			X	X												
	infrared jamming flares			X														
	chaff dispenser			X														
	missiles and rockets	X			X	X												

In addition to empirically testing the design principles against the validated survivability features of the Blackhawk, three additional empirical tests were conducted using the A-10A Warthog (Appendix A), F-16C Fighting Falcon (Appendix B), and Iridium satellite communications network (Appendix C). In tracing the initial design principles to the survivability features of the A-10A (which was conducted in parallel with the Blackhawk empirical test), similar insights emerged (*e.g.*, need to clarify redundancy, need to decompose diversity). Following the F-16C and Iridium empirical tests, no further modifications or refinements were required of the design principle framework.

4.4. Validated Set of Seventeen Design Principles

Utilizing the four-step approach described in the preceding section, seventeen survivability design principles were enumerated. These are classified as six design principles for Type I survivability, nine design principles for Type II survivability, and two design principles for Type III survivability.

4.4.1. Type I (Reduce Susceptibility)

The six principles for enhancing Type I survivability *(i.e.*, susceptibility reduction) are: (1.1) prevention, (1.2) mobility, (1.3) concealment, (1.4) deterrence, (1.5) preemption, and (1.6) avoidance.

Prevention is *the suppression of a future or potential future disturbance.* Through the prevention design principle, disturbances are not given the opportunity to become a threat to the system. An example of prevention is the suppression of enemy air defense (SEAD) before a conflict, intended to remove threats to friendly aircraft.

Mobility is *relocation to avoid detection by an external change agent.* Through the mobility design principle, the disturbance agent's ability to effectively observe the system is diminished because the system is changing locations, thereby making a decision to attack the system more difficult. Examples of the principle include the Navy TACAMO E-6 strategic communications aircraft which is constantly changing locations to avoid detection, and the Scud launcher vehicles, which were often relocated during the first Gulf War conflict to confound U.S. forces attempting to destroy them.

Concealment is *the reduction of the visibility of a system from an external change agent.* Through the concealment design principle, the disturbance agent's ability to effectively observe the system is diminished because the system is difficult to identify or isolate, thereby making a decision to attack the system more difficult. Examples of the principle include the B-2 Spirit stealth bomber and the F-117 Nighthawk stealth aircraft. In addition to minimizing the ability of external change agents to identify systems, concealment may be also employed in a deceptive manner to minimize the ability of agents to isolate systems (*e.g.*, decoys).

Deterrence is *the dissuasion of a rational external change agent from committing a disturbance*, increasing the perceived costs above the perceived benefits of an attack. Through the deterrence design principle, the disturbance agent is convinced not to carry out the disturbance. An example of the principle is the policy of Mutually Assured Destruction pursued during the Cold War. Opponents realized that any action would cause an effect of such high cost that any benefit received would not make the action worthwhile.

Preemption is *the suppression of an imminent disturbance.* Through the preemption design principle, the disturbance agent's ability to act is removed or diminished immediately prior to committing the act. An example of the preemption principle is the interception of hostile missiles, whether immediately before launch or during flight.

Avoidance is *maneuverability away from a disturbance.* Through the avoidance design principle, the disturbance agent's action is reduced in effectiveness through the system actively relocating. Examples include aircraft missile evasion and precision landing of robotic exploration vehicles on Mars.

4.4.2. Type II (Reduce Vulnerability)

The nine principles for enhancing Type II survivability (*i.e.*, vulnerability reduction) are: (2.1) hardness, (2.2) redundancy, (2.3) margin, (2.4) heterogeneity, (2.5) distribution, (2.6) failure mode reduction, (2.7) fail-safe, (2.8) evolution, and (2.9) containment.

Hardness is *the resistance of a system to deformation.* Through the hardness design principle, the system is able to resist more of the effects of a disturbance by raising the intensity required to have negative effects on the system. Examples include Milstar satellite radiation hardening and the M1 Abrams tank armor.

Redundancy is *the duplication of critical system functions to increase reliability.* Through the redundancy principle, the system reduces the effectiveness of a disturbance by requiring multiple failures to achieve the same effect as a disturbance on a non-redundant system. Examples include back-up GEO communications satellites and the Space Shuttle avionics system of five identical general-purpose computers.

Margin is *the allowance of extra capability for maintaining value delivery despite losses.* For example, the A-10 combat aircraft has lift margin with its long, low-set wings that are able to maintain flight even when missing half of a wing. The A-10 also has propulsion margin with an ability to survive the loss of one of its two engines.

Heterogeneity is *variation in system elements to mitigate homogeneous disturbances.* Through heterogeneity, systems reduce the aggregate impact of a single type of disturbances. For example, heterogeneous operating systems have been proposed to reduce the effectiveness of malware. An example of an operational system using heterogeneity as a design principle to improve survivability is the nuclear "triad" of land-based ICBM's, airborne bombers, and nuclear submarines.

Distribution is *separation of critical system elements to mitigate local disturbances.* For example, in order to realize the survivability benefits of redundant flight controls on the A-10, the two mechanical assemblies are functionally and spatially separated.

Failure mode reduction is *the elimination of system hazards through intrinsic design.* Such hazards might be eliminated through component substitution (*e.g.*, following Apollo 13, the replacement of Teflon insulation in the oxygen tanks with stainless steel), design simplification (*e.g.*, reliance on flight-proven hardware), decoupling of failure modes (*e.g.*, placing critical code in read-only memory), and through the reduction of hazardous materials (*e.g.*, using hybrid propulsion systems in place of solid propellant) (Leveson 1995).

Fail-safe is *the prevention or delay of system degradation by leveraging the physics of incipient failure.* Fail-safe designs may eliminate immediate danger by automatically compensating for failure. Several examples of fail-safe are discussed in the Blackhawk test case in Section 4.3.3 (*e.g.*, autorotation of rotor blade).

Evolution is *the alteration of system elements to reduce disturbance effectiveness (engineered mismatch).* Through the evolution design principle, the system actively changes itself to reduce the effectiveness of a disturbance. As discussed in Section 4.2.1, the B-17 design and tactics evolved extensively over the course of the Second World War.

Containment is *the isolation or minimization of the propagation of failure.* For example, the Blackhawk helicopter reduces the risk of hydraulic fluid fires by incorporating quick disconnects and leak isolation valves in the flight control system.

4.4.3. Type III (Enhance Resilience)

The two principles for enhancing Type III survivability (*i.e.*, resilience enhancement) are: (3.1) replacement and (3.2) repair.

Replacement is *the substitution of system elements to improve value delivery.* Through the replacement principle, the system is restored through the substitution of an undamaged element for a damaged component. An example is the launch of XM-3 and XM-4 satellite radio satellites to replace XM-1 and XM-2 due to solar panel fogging that reduced Boeing 702 satellite lifetimes from fifteen to six years.

Repair is *the restoration of a system to an improved state of value delivery.* Through the repair principle, the system is restored through a modification of damaged components to a less damaged state. An example is the STS-61 mission placing Corrective Optics Space Telescope Axial Replacement (COSTAR) on the Hubble Space Telescope in 1993.

4.5. Synthesis

The process of tracing survivability features of real systems to the design principles and the subsequent improvements and eventual validation of the theory illustrates the value of empirical research in systems engineering. As a first step, development of the survivability framework and principles benefited from a deductive approach that emphasized an abstract theoretical framework. Following the generation of a set of hypotheses (*i.e.*, the initial twelve design principles), experiments were conducted (*i.e.*, tracing of survivability features of existing systems to design principles). Based on the results of the experiments, new hypotheses were proposed (*i.e.*, new sets of design principles) for subsequent testing.

Based on the results of the experimentation, the seventeen general design principles in Table 4-7 are found to characterize all of the survivability features employed by four existing, survivable aerospace systems: F-16C, Iridium, A-10A, and UH-60A. Given the stratified sampling of these systems across the aerospace domain, it may be argued that the seventeen design principles constitute a complete framework for informing concept generation of survivable aerospace systems during front-end design activities. The modifications made to the preliminary set of principles (Table 4-3) enable consideration of a larger set of survivability techniques. Capturing the subtle functional differences among design principles also expands the potential design space enumerated from form-function mapping in conceptual design.

Table 4-7. Validated Set of Survivability Design Principles

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

Figure 4-5 depicts the time intervals during which each of the seventeen design principles may positively affect value delivery in a disturbance lifecycle. Principles enhancing Type I survivability add value before a disturbance impacts a system, Type II principles add value during the disturbance, and Type III principles add value following a disturbance impact. While the design principles are helpful for aiding the creative brainstorming of a larger set of survivability techniques in each phase of a disturbance, they are not intended as a checklist 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.

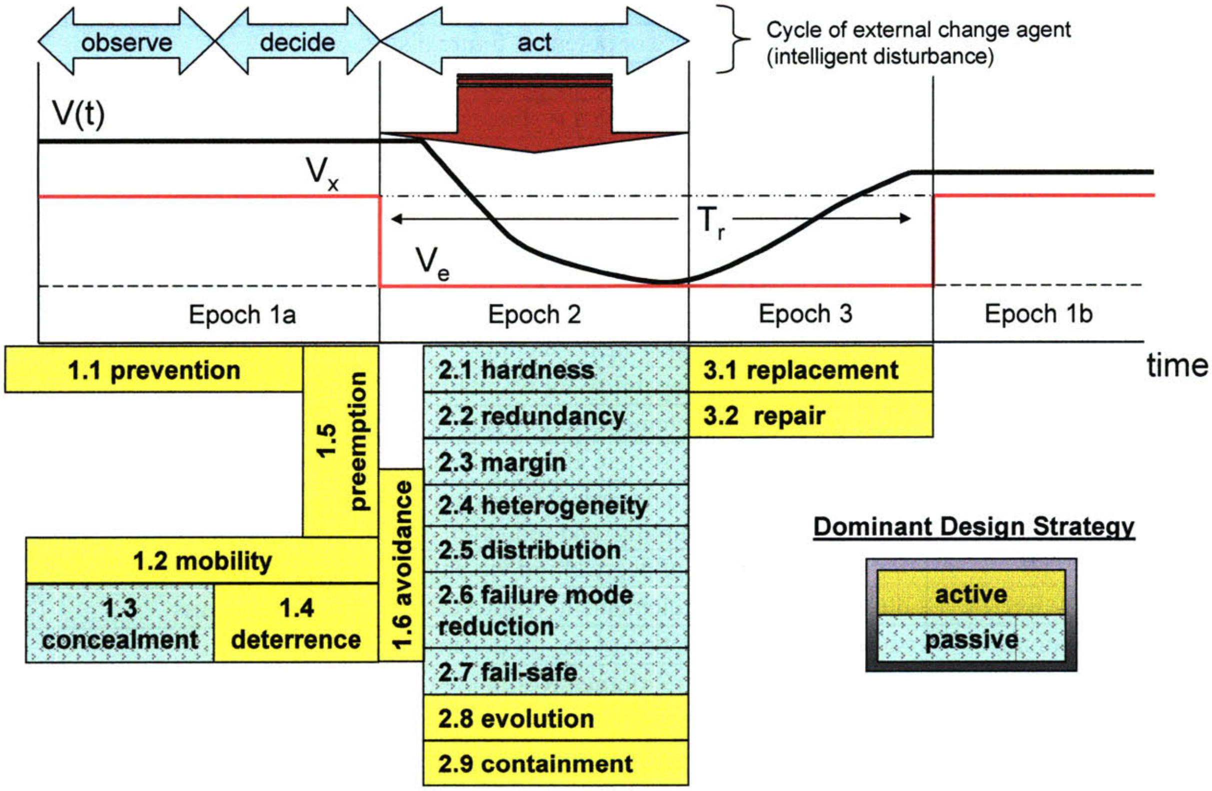


Figure 4-5. Mapping of Design Principles to Disturbance Lifecycle

As illustrated in Figure 4-5, each design principle is classified as either passive or active. A focus on passive principles will lead to the construction of closed (static) systems that resist disturbance based on projections of the operational environment. A focus on active principles will lead to the construction of open (dynamic) systems that cope with future uncertainty by stressing architectural agility to recover from disturbances (Table 4-8). The distinction between passive and active survivability is useful because it specifies which design principles may be used based on the changeability of the architecture (Ross 2006). For example, the current generation of communications satellites has a low degree of changeability due to the inaccessibility of the orbiting vehicles following launch. In order to achieve survivability in the harsh environment of space, designers focus on the passive design principles of radiation hardening and redundancy (increasing mass, complexity, and cost). If on-orbit servicing vehicles were to be developed, the changeability of communications satellites would increase. This would provide designers the option of incorporating design principles of active survivability such as repair, replacement, and evolution via servicing missions in lieu of costly hardening and radiation techniques (Richards 2006).[24]

Table 4-8. Passive vs. Active Survivability

	Passive Survivability	**Active Survivability**
Philosophy	Survivability is something that a system *has*	Survivability is something that a system *does*
Characteristics	proactive, resistant, robust	reactive, flexible, adaptive
Design Principles	concealment, hardness, redundancy, margin, heterogeneity, distribution, failure mode reduction, fail-safe	prevention, mobility, deterrence, preemption, avoidance, evolution, containment, replacement, repair
Forecasting	Presupposes knowledge of disturbance environment	Acknowledges uncertainty in projection of future disturbances
Architecture	Closed (static)	Open (dynamic)
Design Focus	Defensive barriers at system-level to resist disturbances	Architectural agility to deter, avoid, and/or recover from disturbances
Failures	Causal chain (often linear)	Tight couplings, functional resonance (nonlinear)
Related Disciplines	Safety engineering, risk analysis	Operations analysis, real options analysis

Table 4-8 describes how the design principles may be broadly decomposed into passive (structural) principles that seek to maintain value delivery through static design elements and active (behavioral) principles that focus on either eliminating disturbances or on agile architectures for rapid recovery. However, it is important to note that the passive/active attributes of the design principles are not absolute distinctions but rather representative of a continuum between two different design philosophies. For example, concealment is not amenable to this binary categorization as many concealment features on combat aircraft are active in nature (*e.g.*, chaff and flare dispensers). These features require situational awareness, decision-making, and action by the pilot (*i.e.*, the ODA cycle of the internal change agent).

The scope of this chapter—the development of a validated set of survivability design principles—is only one aspect of improving the articulation, evaluation, and implementation of survivability during the conceptual design of engineering systems. The next step is a

[24] Changeability may also serve as an enabler of active survivability in space systems through internal, adaptive system behavior (rather than through the external, flexible changes offered by on-orbit servicing). For example, self-similar modular architectures enable reconfigurability which accommodates graceful degradation (Siddiqi and De Weck 2006) through the survivability design principles of *containment* and *repair*. Each of these architectural properties related to changeability—whether classified as flexible, adaptable, or reconfigurable—serve as path enablers of survivability by reducing the time and/or costs associated with exercising various combinations of active survivability design principles.

quantitative implementation of the principles into a system analysis methodology. In the following chapter, the survivability metrics from Chapter 3 are applied to a series of tradespace computer experiments for comparing designs on the basis of their lifecycle cost, design utility, and survivability. Having demonstrated this modeling approach, a methodology is introduced in Chapters 6 and 7 for using the design principles to expand the set of system design trade-offs under consideration.

5. Survivability Tradespace Experiments

This chapter addresses the third of the four research questions introduced in Section 1.3.2.

3. How can survivability be quantified and used as a decision metric in exploring tradespaces during conceptual design of aerospace systems?

The objective of this chapter is to examine the survivability metrics introduced in Chapters 2 and 3 through their application to a series of computer experiments. Drawing upon both existing and proposed metrics, the ability of each metric to specify, evaluate, and verify survivability in trade studies during conceptual design is analyzed. (As discussed in Section 2.2, trade studies are analyses that evaluate a range of design options in terms of costs and benefits.) The computer experiments are focused on establishing the internal validity of the survivability metrics. Therefore, systems were selected for testing the survivability metrics for which threats and mitigating strategies are well-documented. Subsequent application of the metrics in Chapter 7 is focused on testing for external validity by seeking prescriptive insights.

Five desirable characteristics for conducting survivability assessments are used to evaluate the approach taken by each computer experiment. First, does the methodology allow survivability to be actively traded with traditional measures-of-effectiveness (*e.g.*, lifecycle cost, mission utility)? Second, are the dynamics of hostile operational environments incorporated into survivability considerations over the entire lifecycle? Third, are path-dependencies associated with system state internalized? Fourth, is survivability considered at the architectural level? Fifth, does the methodology take a value-centric approach to allow alternative value-delivery mechanisms in the tradespace, ensuring that the survivability analysis is focused on the preservation of mission utility (vice physical integrity of constituent nodes)?

These five questions are answered in each of Chapter 5's three survivability test cases. In Section 5.1, cost-exchange ratios (*i.e.*, evaluating system survivability in terms of optimizing a defensive system's cost-exchange ratios with the attacker) are evaluated through their application to a simple model of space-based ballistic missile defense (BMD). In examining this existing approach to the front-end evaluation of survivability, general findings for space-based BMD are also discussed. In Section 5.2, existing survivability metrics are applied to an emerging tradespace methodology. In particular, survivability considerations are incorporated into a Multi-Attribute Tradespace Exploration study of an orbital transfer vehicle operating in a debris environment. Limitations of the existing survivability metrics and static MATE methodology applied in this study are used to inform Section 5.3, where the MATE analysis of orbital transfer vehicles is extended and customized to accommodate the dynamics and path dependencies associated with assessing survivability as a stochastic property across the system lifecycle. Both existing and proposed survivability metrics are applied to the computer experiment. Section 5.4 summarizes the lessons learned and draws general conclusions from the three computer experiments.

5.1. Test Case #1: Cost-Exchange Ratios

The Nitze criterion was introduced in Section 2.1.3 as one accepted means for assessing novel defenses. The central tenet of the Nitze criterion is that defenses are worth deploying if they are more cost-effective at the margin (*i.e.*, recurring cost of defense is less than the recurring cost of the countermeasures that could be used against the defense). System analyses applying the Nitze criterion therefore focus on calculating the cost-exchange ratios associated with attack, countermeasures, and counter-countermeasures. This section revisits the work of Canavan and Teller (1990) in applying the Nitze criterion to evaluate alternative survivability enhancement features for a space-based ballistic missile defense (BMD) system. Since the technical issues involving the first-order survivability of space-based BMD are well-documented (Canavan and Teller 1990), this test case applies existing assumptions to build a simple model of space-based BMD. Accordingly, the focus of the analysis is on the strengths and weaknesses of using cost-exchange ratios as a decision metric.

Following a brief overview of space-based BMD and discussion of survivability considerations, a parametric, first-order model of space-based BMD is developed to assess a tradespace of candidate defensive alternatives. Interrelationships between cost, performance, and survivability of systems pursuing alternative strategies are explored. The section concludes with general comments on space-based BMD and a synthesis of lessons learned from employing cost-exchange ratios for front-end survivability assessments.

5.1.1. Overview: Space-Based Ballistic Missile Defense

The utilization of space-based interceptors to protect the United States and its allies from ballistic missile attack has been the subject of decades of research and development activities. Beginning with the Defense Advanced Research Projects Agency's Project Defender in the 1960's, several candidate systems have been proposed. In the early 1990's, the Global Protection Against Limited Strikes (GPALS) system envisioned a constellation of several thousand "Brilliant Pebbles" that would provide boost and early mid-course defense against ballistic missile launches from all over the world (Blaha, Pendergraft and Riley 2007). Although abandoned for political and economic reasons (*e.g.*, post-Cold War peace dividend, desire to maintain 1972 Anti-Ballistic Missile Treaty with the former Soviet Union), GPALS reached a high level of technical maturity. Over the past decade, the world situation has further evolved and a strong value proposition for space-based BMD may be made by proponents in terms of technology (*e.g.*, ability to track missile launches in boost-phase, difficulty for offense to deploy countermeasures in boost-phase relative to midcourse phase), safety (*e.g.*, desire to intercept nuclear-tipped missiles over hostile territory), geopolitics (*e.g.*, increased number of hostile nations seeking ballistic missiles, heightened pace of proliferation of missile technology, recent North Korean tests), funding availability (*e.g.*, burgeoning U.S. Missile Defense Agency budget), legality (*e.g.*, 2002 withdrawal of U.S. from ABM Treaty), and political support (*e.g.*, 2002 National Security Policy Directive 23 which directed the development and testing of a space-based defense).[25] Despite these arguments, a host of issues remain (*e.g.*, potential to militarize space in a way that damages U.S. interests in the long-term) (O'Hanlon 2004; Rance 2007). The issue explored in this section focuses on the efficacy of space-based BMD given the countermeasures that can be deployed against it: how to make such a system survivable?

[25] A host of arguments have also been made against space-based BMD in terms of technology and national security strategy (Stares and Pike 1985; Pike 1986; Canavan and Teller 1990; DeBlois 2004; Wright, Grego and Lisbeth 2005)

Described as "the crowning achievement of the Strategic Defense Initiative" by former Lawrence Livermore National Laboratory Director John Nuckolls, the Brilliant Pebbles were a set of non-nuclear watermelon-sized mini-missiles designed to kinetically intercept and kill ballistic missiles in the boost and early mid-course phases of flight. Without accounting for survivability considerations, the Brilliant Pebbles were shown to have highly-effective cost-exchange ratios with Soviet ICBMs when deployed in carrier vehicles (Canavan and Teller 1990; Canavan 1991). However, when accounting for countermeasures, absenteeism, and cost-effectiveness relative to other defense strategies (*e.g.*, hardening, decoy and maneuver), the Brilliant Pebbles embraced a distributed singlet architecture (*i.e.*, one interceptor per carrier vehicle) for achieving favorable cost-exchange ratios with the attacker. In examining the strengths and weaknesses of using cost-exchange, the computer experiment in this section will return to and attempt to build on these previous assessments of how to best achieve a survivable space-based BMD system.

5.1.2. Survivability Considerations

Candidate kinetic-kill space-based BMD systems suffer from many susceptibilities and vulnerabilities characteristic of most spacecraft as well as unique fragilities arising from the nature of their mission (*e.g.*, global coverage, immediate response time). As discussed in Wheelon (1986), space systems are subject to attack. For one, target acquisition may be conducted by direction finding from emissions of electromagnetic radiation, passive infrared sensing of electrical energy against the backdrop of space, or microwave radar or laser tracking. Once targets are acquired, satellites may be tracked given the predictability of their orbits and ΔV penalties associated with maneuvering, particularly in low Earth orbit (LEO). Wheelon also notes that destroying LEO satellites is not difficult given that it is only necessary to stand in their path to destroy them given high relative velocities. Of course, kinetic attacks are not the only disturbances against which a potential space-based BMD would need to contend. Several other potential hazards are documented in the literature (Giffen 1982; Wheelon 1986; Hastings and Garrett 1996; Wilson 2001; Tribble 2003).

In addition to recognizing the generic threats facing any space system, it is also important to recognize the unique fragilities introduced by the space-basing of missile defense. First, interceptors must be in LEO in order for the defender to be within a distance equal to the product of its velocity and the time its takes the attack missile to accelerate to ballistic trajectory (*i.e.*, before the discriminatory targeting problem brought about by decoys arises) (Canavan and Teller 1990). This constraint forces systems to be at 500 km or less in altitude (Canavan and Teller 1990). Furthermore, such systems must be somewhat distributed in order to account for absenteeism—a factor of approximately 20% which is driven by the defenders velocity (Canavan and Teller 1990). Therefore, the space-based BMD architectures in the tradespace will consist of a thin shell of satellite carrier vehicles in LEO holding one or more interceptors (where n=1 in case of Brilliant Pebbles).

Given the susceptibility and vulnerability of LEO space systems and the unique fragilities arising from the space-based BMD mission area, what survivability features might be deployed to increase the efficacy of a future system? While all seventeen principles offer options for architectural improvement, this section examines the impacts of increasing the number of interceptors available over a given field of regard (*margin*) and decreasing number of interceptors per carrier vehicle (*distribution*).

5.1.3. Tradespace Analysis

In order to analyze the survivability of alternative missile defense systems, a two-step modeling effort is pursued. First, a baseline space-based BMD system is designed to understand the minimum number of interceptors required on-orbit to maintain a high-degree of confidence in a leak-proof defense (*i.e.*, >95% probability of intercepting all hostile missile launches) within a reasonable budget. Second, the impact of distributing the BMD architecture over multiple carrier vehicles is modeled in the event that an adversary pursues countermeasures (rather than simply launching more missiles). Trade-offs are examined among a Brilliant Pebbles (*i.e.*, singlet) system and less distributed BMD systems using carrier vehicles with multiple interceptors. Sensitivity analysis is conduced on the most critical assumptions and the computer experiment concludes with a discussion on how other design principles (*e.g.*, hardening) may be added to the tradespace for a more complete assessment of survivability.

The purpose of modeling a baseline space-based BMD system is to understand the relationship between the number of interceptors within a given field of regard and a target performance level of the system (*i.e.*, the probability of a leak-proof defense against a limited hostile launch). As such, the first-order model allows trades between desired performance and investment in additional interceptors.

There are two independent variables in this baseline case: (1) the number of total interceptors deployed and (2) the anticipated number of rounds of launch. The second independent variable reflects the CONOPS of the BMD (*i.e.*, the number of rounds of ICBMs launches across which defensive interceptors are allocated). Thirty design vectors are considered, representing the full-factorial sampling of the two design variables.

- number of interceptors deployed in LEO [10 30 60 100 150 225 350 500 750 1000]
- anticipated number of rounds of launch [1 2 3]

Having generated design alternatives, a simple model translates each design vector into the performance parameters of the probability of a leak-proof defense (per round) and the cost of defense. Given that the focus of this section is on the implications of using cost-exchange ratios for survivability analysis, the assumptions and governing equations underlying the simple model are provided in Appendix D.

Figure 5-1 shows the baseline space-based BMD tradespace, displaying the performance of the thirty design alternatives. The costs of the systems vary from 10 to 40 billion dollars, and the probability of a leak-proof defense (against a three-missile salvo from any point on the Earth's surface) ranges from less than 10% to performance in excess of 0.99 probability.

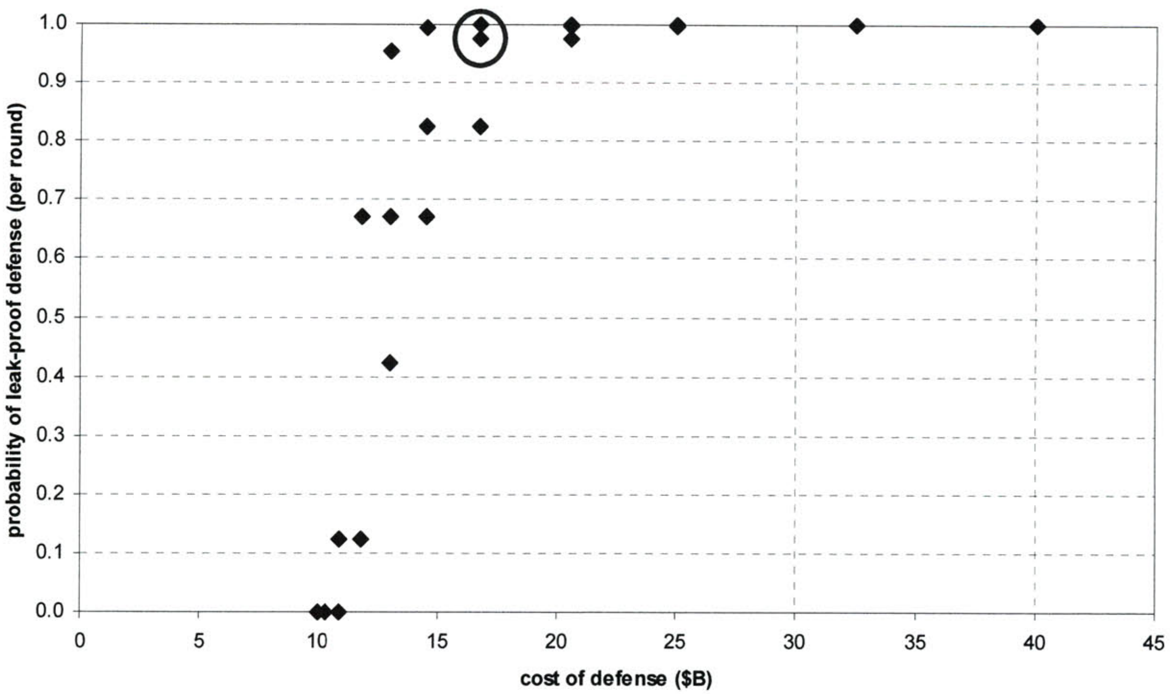
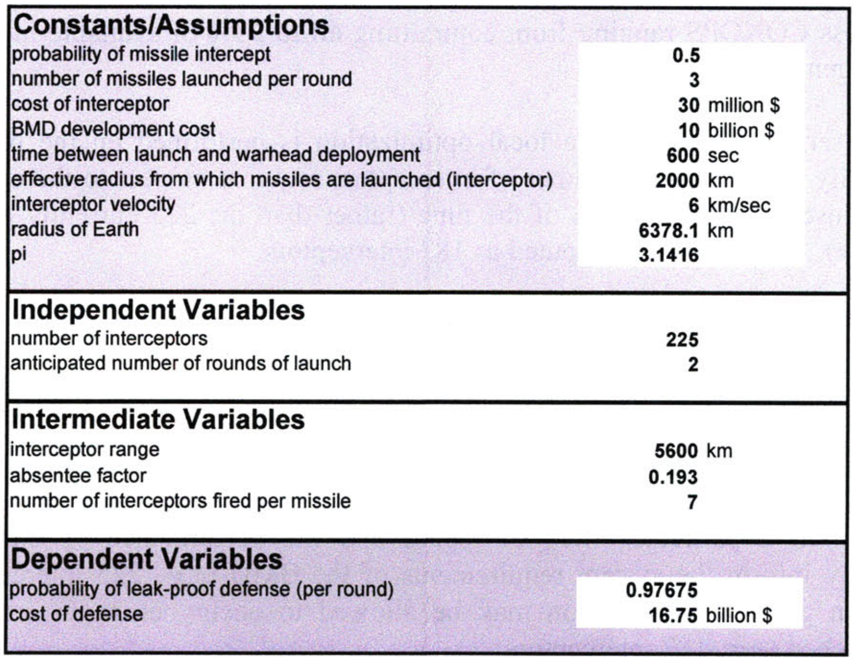


Figure 5-1. Baseline Space-Based BMD Tradespace

Table 5-1 shows a promising baseline architecture (circled in Figure 5-1) given its high probability of leak-proof defense and (relatively) low cost.

Table 5-1. Promising Point Design for Baseline Space-Based BMD



Constants/Assumptions		
probability of missile intercept	**0.5**	
number of missiles launched per round	**3**	
cost of interceptor	**30**	million $
BMD development cost	**10**	billion $
time between launch and warhead deployment	**600**	sec
effective radius from which missiles are launched (interceptor)	**2000**	km
interceptor velocity	**6**	km/sec
radius of Earth	**6378.1**	km
pi	**3.1416**	
Independent Variables		
number of interceptors	**225**	
anticipated number of rounds of launch	**2**	
Intermediate Variables		
interceptor range	**5600**	km
absentee factor	**0.193**	
number of interceptors fired per missile	**7**	
Dependent Variables		
probability of leak-proof defense (per round)	**0.97675**	
cost of defense	**16.75**	billion $

Having identified a promising design, a sensitivity analysis was conducted on the CONOPS to explore the implications of alternative tactics on architecture performance (Figure 5-2).

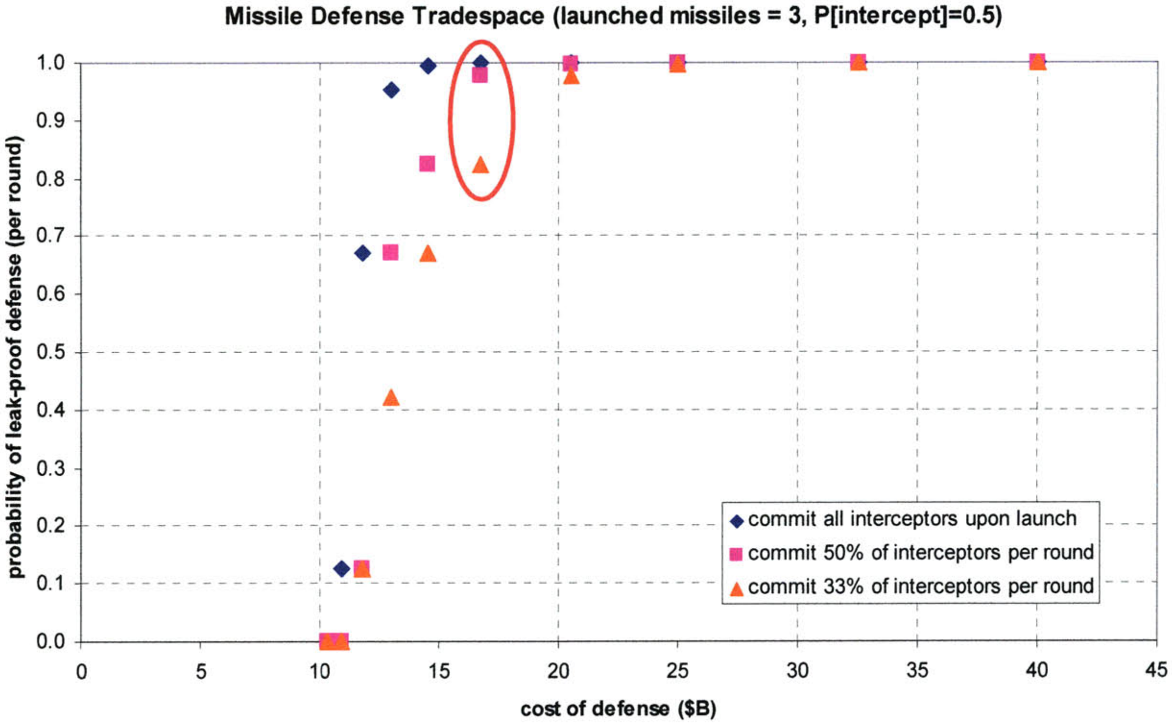


Figure 5-2. Sensitivity Analysis on Assumed BMD CONOPS

As illustrated by the encircled points in Figure 5-2, the baseline architecture is reasonably survivable across CONOPS ranging from committing all to 33% of available interceptors for a particular engagement.

Following the sensitivity analysis, a local optimization is performed on the promising point design to identify the minimum number of interceptors required subject to the constraint that a leak-proof defense is delivered 95% of the time (rather than the 225 currently employed for a 98% probability). That value is computed as 187 interceptors.

Before proceeding, it is important to note the first-order nature of the calculations performed above. While first-order parametric models are useful for depicting relative trends, it would be unwise to extract general results without higher fidelity models, improved cost estimates, and more complete sensitivity analysis on the extensive number of assumptions (*e.g.,* probability of missile intercept, interceptor velocity, ICBM launch time). Nevertheless, the model is adequate for our purpose of roughly estimating the relationship between the number of available interceptors within a particular field of regard and the performance of the BMD. This relationship may inform the system requirements of the BMD (*e.g.*, 225 interceptors) and the extent to which graceful degradation may be allowed to occur before an emergency value threshold is reached (*e.g.*, 187 interceptors).

Having established a required baseline capability for the space-based BMD in terms of the number of interceptors required within a particular field of regard, the impact of countermeasures against the defensive interceptors is examined. The published model of Canavan and Teller (1990) is applied to explore the tradeoff between distributed and concentrated BMD architectures when an ICBM launch is preceded by a direct-ascent attack designed to "poke a hole" in the "umbrella" of interceptors. The particular scenario examined in this case is ten direct-ascent weapons launched at BMD carrier vehicles prior to launch of three ICBMs. Assumptions made regarding the marginal cost of attack are documented in Appendix D. Defender costs are carried through the calculations as mass on-orbit before being later converted to a dollar value assuming a $10,000/kg launch cost.

To examine trade-offs among a Brilliant Pebbles (*i.e.*, singlet) system and other BMD systems using carrier vehicles with multiple interceptors, two design variables are considered: (1) number of carrier vehicles and (2) number of interceptors per carrier vehicle. An important intermediate variable calculated in the analysis is the mass of a carrier vehicle, which is calculated in Canavan and Teller (1990) as a function of the number of interceptors (n):

$$MassCarrier = 100n^{2/3} \tag{5-1}$$

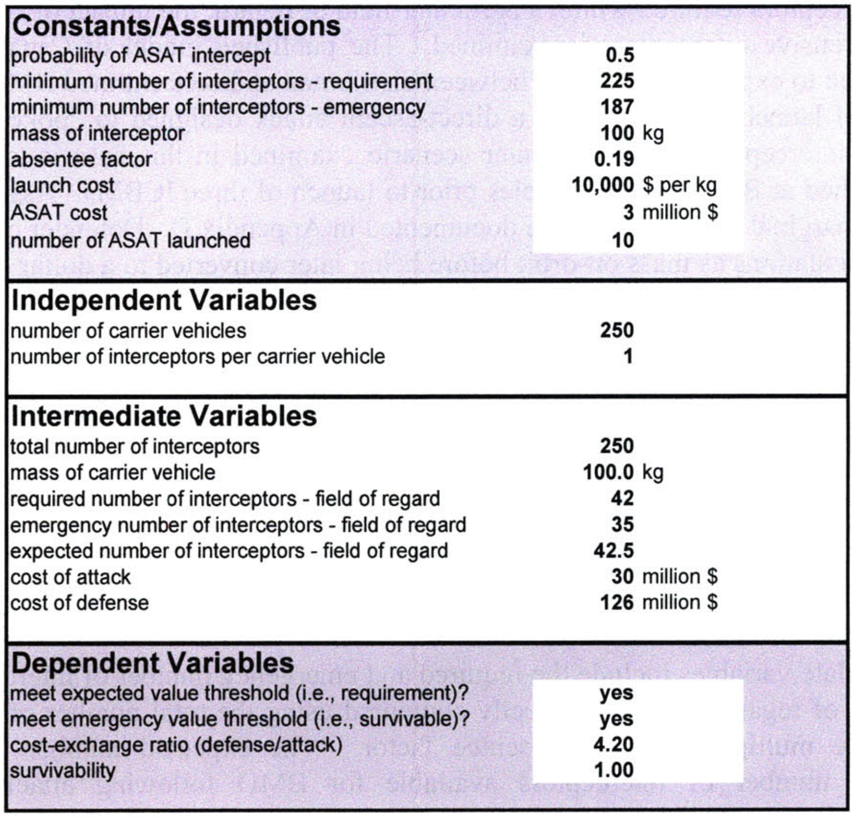
Other intermediate variables include the required and emergency number of interceptors within a particular field of regard. Both are directly computed using the total number of interceptors in the architecture multiplied by the absentee factor. The expected number of interceptors represents the number of interceptors available for BMD following attack. Using the formulation by Howard (1993), this value is computed as the difference between the number of available interceptors within the field of regard and the number of interceptors eliminated by anti-satellites:

$$ExpNumInt = TotalInt * Absentee - NumASAT * EffectASAT * NumIntPerCV \tag{5-2}$$

Next, the cost of defense is computed as the redundant capability launched on-orbit as margin in the BMD constellation. Specifically, it is computed as a function of the mass of any interceptor (and associated carrier vehicle) launched in excess of those needed to meet the performance requirement (*i.e.,* 225 interceptors).

Four dependent variables are computed, two binary and two continuous. The first two consists of logic tests regarding the architectural performance (Is the expected value threshold met? Is the emergency value threshold met?). The subsequent two compute the ratio of the cost of defense to the cost of the offense and survivability. A survivability index is assumed to be 1 if the expected value threshold is met, 0 if the emergency value threshold is not met, and linearly scaled for intermediate cases.

Table 5-2. "Brilliant Pebbles" Point Design of 235 Singlets



Constants/Assumptions		
probability of ASAT intercept	**0.5**	
minimum number of interceptors - requirement	**225**	
minimum number of interceptors - emergency	**187**	
mass of interceptor	**100**	kg
absentee factor	**0.19**	
launch cost	**10,000**	$ per kg
ASAT cost	**3**	million $
number of ASAT launched	**10**	
Independent Variables		
number of carrier vehicles	**250**	
number of interceptors per carrier vehicle	**1**	
Intermediate Variables		
total number of interceptors	**250**	
mass of carrier vehicle	**100.0**	kg
required number of interceptors - field of regard	**42**	
emergency number of interceptors - field of regard	**35**	
expected number of interceptors - field of regard	**42.5**	
cost of attack	**30**	million $
cost of defense	**126**	million $
Dependent Variables		
meet expected value threshold (i.e., requirement)?	**yes**	
meet emergency value threshold (i.e., survivable)?	**yes**	
cost-exchange ratio (defense/attack)	**4.20**	
survivability	**1.00**	

Table 5-2 illustrates a "Brilliant Pebbles" point design in the parametric model that calculates the survivability and defense-offense cost-exchange ratios for various BMD architectures. This particular architecture—the Brilliant Pebbles singlet case of n=1 when 250 interceptors are deployed—exceeds both the emergency and expected value thresholds with the lowest cost-exchange ratio.

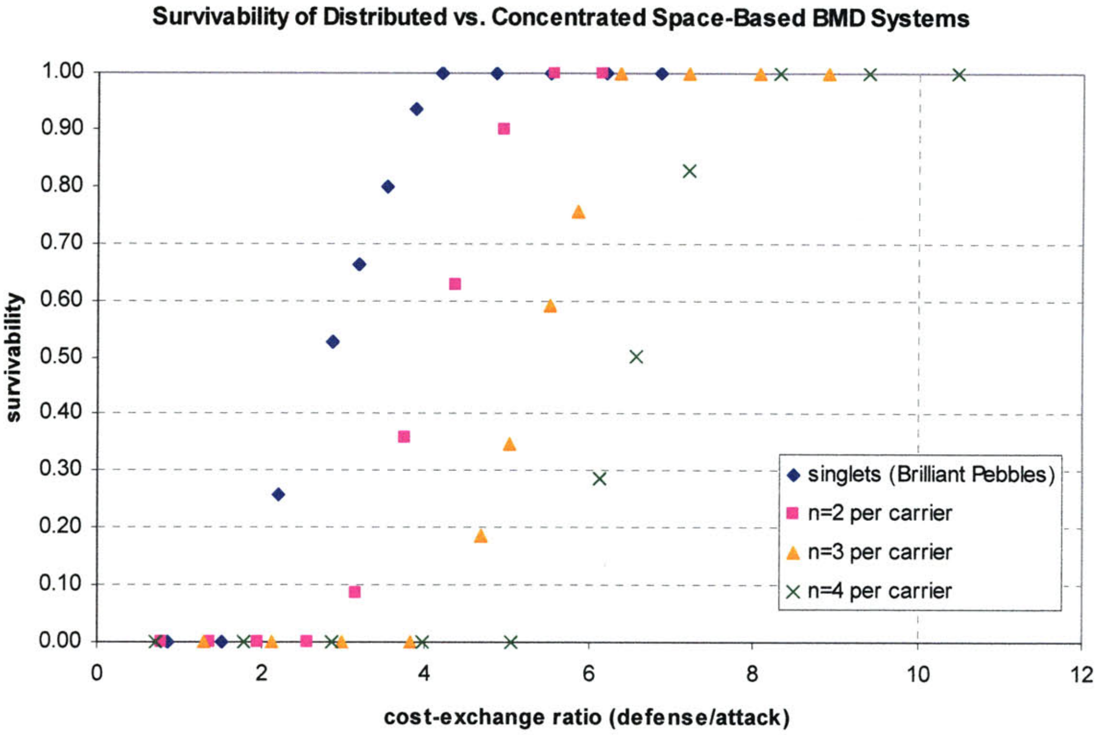


Figure 5-3. Survivability as a Function of Cost-Exchange Ratios

Figure 5-3 illustrates the survivability of all 45 candidate architectures as a function of the cost-exchange ratio with the offense. This figure is consistent with the proponents of space-based BMD who argue that the only survivable missile system is a Brilliant Pebbles configuration. Another interesting result of this figure is the fact that all architectures which achieve at least a 95% probability of leak-proof defense (which is any point in Figure 5-3 that has a non-zero survivability value) have a cost-exchange ratio with the offense of at least two. This means that, in a strict application of the Nitze criterion, no redundant "Pebbles" should be launched because the cost-exchange ratio favors the attacker. However, a more narrow interpretation of the Nitze criterion applied to the simple model might be that all configurations incorporating more than one interceptor per carrier vehicle should be dismissed as dominated solutions.

As in the preceding case of establishing the baseline space-based BMD system, the trade-offs presented in this computer experiment are only of a first-order nature and require higher-fidelity models before specific implications for Brilliant Pebbles might be argued. For example, is it true that a decision-maker would only be willing to accept a leak-proof missile defense system if the probability of completely successful intercepts is 95%? Such assumptions bound the computation of survivability in Figure 5-3.

5.1.4. Key Insights

> *"Bacteria, polyps, ants, and bees are the living proof that, given inhospitable conditions, colonies stand a better chance of survival than individuals....A colony of microsatellites will be less vulnerable than a normal satellite, not only to gamma radiation and solar storms, but also to cutbacks" (Van Kasteren 2004).*

Three general conclusions may be drawn for space-based BMD from the first-order model. First, redundant constellation nodes are expensive mechanisms for making satellite capabilities insensitive to attack given the large cost of mass on-orbit. Second, as previously advocated (by Canavan, Teller, and Lowell), it is wise to distribute capability over as many spacecraft as possible to minimize cost-exchange ratio with a potential attacker. Third, maximizing the allowable loss of interceptors within a particular field of regard may enable non-catastrophic, graceful degradation of a BMD constellation. Possibilities for future work include exploring the impact of maneuver tactics on cost-exchange ratios with homing attack vehicles, exploring the impact of radiation hardening carrier vehicles on cost-exchange ratios with nuclear weapons, and modeling the uncertainty of the attacker (*e.g.*, unknown BMD survivability features) and defender (*e.g.*, unknown scope and magnitude of BMD countermeasures) to consider a wide-range of possible future engagements and to compute the value of perfect information on both sides.

In addition to general findings regarding space-based BMD, insights from the simple test case also include implications of utilizing cost-exchange ratios in survivability analysis. These implications are discussed in terms of the five desirable criteria provided in the introduction of Chapter 5. First, applying cost-exchange ratios to parametric computer models does allow survivability to be traded with relative costs. However, in a assuming a baseline system, it is not possible to directly trade system performance and survivability. Second, the test case fails to incorporate the dynamics associated with a particular threat encounter or lifecycle performance by relying on a deterministic assessment of mission utility. Third, while cost-exchange ratios are useful for thinking through the strategic interactions between attacker and defender behavior, the test case failed to internalize path dependencies in system-state. Fourth, the test case successfully demonstrates that cost-exchange ratios can be applied to studies extending to architectural scope by evaluating survivability strategies at the satellite and constellation level.

The fifth and final criterion, providing a value-centric assessment, is partially addressed by translating all offensive and defensive actions into a dollar figure. As discussed in Section 2.1.3, Paul Nitze's criterion of deploying novel defenses if it is more cost-effective at the margin is an intuitively appealing construct. However, cost-exchange ratios may be of limited value if the value of a particular dollar spent on defense is not conserved across actors. This problem may have existed for the space-based BMD system during the Cold War (given the larger size of the U.S. economy relative to the Soviet Union); and this problem of applying the Nitze criterion certainly exists today when discussing the context of conventional military systems facing asymmetric threats. Therefore, while cost-exchange ratios are intuitively appealing and applicable for conducting *relative* tradeoffs among candidate survivability features, they are limited in prescribing absolute tradeoffs of whether to pay for a particular survivability feature.

5.2. Test Case #2: Multi-Attribute Tradespace Exploration

Multi-Attribute Tradespace Exploration (MATE) was introduced in Section 2.2.2 as an emerging conceptual design methodology that applies decision theory to model and simulation-based design (Ross, Hastings et al. 2004). This section explores how survivability metrics can be incorporated into multi-attribute utility tradespaces.

One of the principal challenges of incorporating "-ilities" such as survivability in tradespace studies is the inherent dependencies of the "-ilities". As temporal constructs, the "-ilities" are difficult to represent in a traditionally static tradespace (Section 1.1.4). In addition, since their definition is related to changes in system form or function, they are quantitatively dependent upon other objective function variables. Tradespace studies typically look at the relation between function and/or form and resulting system performance in terms of system objectives. The performance in an aggregated, multi-objective space is dependent on the performance of each of the single objectives. In choosing an appropriate aggregation technique, it is important not to double-count the single objective performances. Incorporating "-ilities", which by definition are measures of the ability to maintain attributes under changing conditions, into a multi-attribute objective function creates the problem of double-counting. Therefore, "-ilities" such as survivability are disaggregated from other system attributes and their impact on the tradespace is assessed independently.

To illustrate the incorporation of survivability into MATE, the survivability of a space tug vehicle operating in low-Earth orbit (LEO) is investigated. The tradespace for this system is simple, well understood, verified, and fairly "rich" in the sense that the "best" system is dependent on the interaction of user needs, environment, and physical constraints in non-trivial ways (McManus and Schuman 2003). The survivability is defined in terms of sustained tug performance in an orbit with an impact threat from micrometeorites and orbital debris. While passive (*e.g.*, hardening) and active (*e.g.*, maneuvering for collision avoidance) survivability strategies exist, this test case focuses on the addition of bumper shielding. Parametrically-varied designs are evaluated for the effect of the shielding on value delivery in a baseline analysis of cost and utility. Survivability is then calculated as the probability of sustaining mission through the threat environment for a ten-year operational life. Since the physical survivability of spacecraft to orbital debris is well-documented (Klinkrad 2006), this computer experiment can utilize existing impact models and focus on the methodological challenges associated with incorporating existing metrics for survivability into a static MATE analysis. Furthermore, the computer experiment can serve to illustrate how adding survivability as a decision metric to lifecycle cost and multi-attribute utility may affect front-end design choices.

5.2.1. Overview: Space Tug

A space tug is a vehicle designed to rendezvous and dock with a space object; make an assessment of its current position, orientation, and operational status; and, then, either stabilize the object in its current orbit or move the object to a new location with subsequent release (Richards, Springmann and McVey 2005). A notional schematic of a space tug is provided in Figure 5-4.

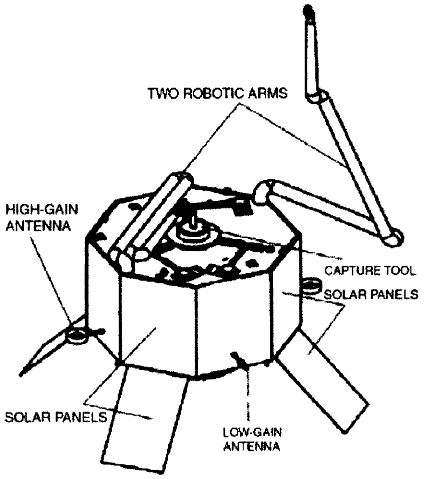


Figure 5-4. Sample Space Tug Configuration (de Peuter, Visentin and Fehse 1994)

A previous MATE study explored the tradespace for a general-purpose servicing vehicle (McManus and Schuman 2003). Three attributes formed the multi-attribute utility function: total ΔV capability, capability of the grappling system, and response time. To provide these attributes, three design variables were considered in subsequent modeling activities: manipulator mass, propulsion type, and fuel load. A full-factorial, design space was sampled and analyzed—featuring 128 designs—by inputting each possible combination of design variables from a set of enumerated values over a range into (1) a parametric cost estimation model and (2) a physics-based performance model. Building on the previous architecture trade study, the MATE model discussed in this section incorporates survivability into the tradespace. Survivability is measured in terms of probability of sustained tug performance in a LEO debris environment for a ten-year mission life. For modeling simplicity, space tugs assume one of two states: operational or non-operational due to catastrophic debris impact.

5.2.2. Survivability Considerations

There are millions of kilograms of objects in Earth orbit that pose a series of challenges to space mission designers. Table 5-3 summarizes the threat to LEO spacecraft by combining data on debris flux from two sources: (1) NASA's EVOLVE breakup engineering model for objects less than 10 cm in diameter (Remo 2005) and (2) empirical data of debris greater than 10 cm in diameter.[26] To provide context to these cross-sectional area flux levels, the total expected number of annual collisions between debris and all operational LEO satellites is also included in Table 5-3 (Lai, Murad and McNeil 2002; UCS 2006).[27] Despite the precision suggested by the calculations in Table 5-3, it is important to note that our ability to understand the actual distribution of debris momentum is dependent upon drawing inferences from a very small set of the overall debris population (Lai, Murad and McNeil 2002).[28]

[26] Published in NORAD's catalog and available for download from Air Force Space Command: http://www.space-track.org/perl/login.pl.

[27] Assumes 10 square-meters as the average exposed surface area of the 352 LEO spacecraft listed in the UCS Satellite Database (Lai, Murad and McNeil 2002).

[28] Given the finite resources available for space situational awareness, a large portion of the estimates of the debris population are susceptible to large sampling errors.

Table 5-3. Cumulative Annual Debris Impact Risk in LEO

Data Source	Object Diameter (cm)	Cross Section Flux (collisions/m^2/year)	LEO collisions/year[29]	Result
(Remo 2005)	0.1	8.0 x 10^{-4}	2.82	Degradation
	0.3	2.0 x 10^{-4}	0.70	Damage
	0.5	1.0 x 10^{-4}	0.35	Damage
	1	4.0 x 10^{-5}	0.14	Severe Damage
Tracked Debris (NORAD catalog)	10	2.5 x 10^{-6}	8.80 x 10^{-3}	Severe Damage
	100	5.0 x 10^{-7}	1.76 x 10^{-3}	Severe Damage
	1000	1.0 x 10^{-9}	3.52 x 10^{-6}	Severe Damage

The environmental hazards posed by orbital debris in LEO lead designers to focus on protection measures for long-lived spacecraft. The amount of damage sustained by a spacecraft is dependent on a variety of factors: debris mass, debris relative velocity, debris shape, debris composition, satellite structure, and location of impact. In general, there are two methods—passive and active—for protecting spacecraft from most debris. Active techniques involve having an awareness of incoming debris threats and a means to avoid or mitigate impact. Passive techniques include shielding, redundancy, and reducing the exposed satellite cross-sectional area signature along the leading edge (the angle-of-attack of most LEO debris) (Wertz and Larson 1999).

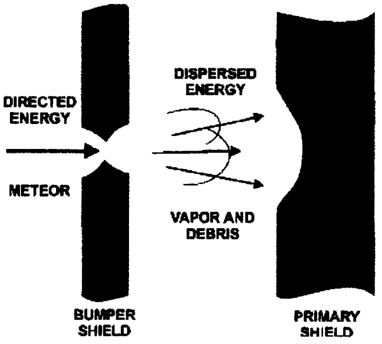


Figure 5-5. Satellite Bumper Shield (Lai, Murad and McNeil 2002)

The model focuses on the protective measure of bumper shielding.[30] Multi-layer bumper shields provide an effective form of passive protection against debris fragments smaller than 1 cm in diameter. Bumper shields provide survivability to spacecraft by fragmenting or vaporizing a projectile in the first layer, dispersing the impulsive projectile into a particle cloud that impact the subsequent shield layers over larger areas (Figure 5-5). The design parameters of a bumper system are the thickness and material of the outer wall, the spacing between the outer wall and backup layers, and the thickness and material of backup layers. The empirically-derived equation for the thickness of the primary shield required for there to be no deflection, rupture, or spalling, t_b, is given:

[29] Assuming a 10 m^2 cross-sectional area for LEO satellites.

[30] Ground-directed active debris avoidance is an expensive proposition as it requires active tracking of co-orbiting objects, additional propellant, coordination with tracking facilities operated by U.S. Space Command, and coordination with spacecraft in adjacent orbits. Also, active collision avoidance is only practical against large objects as ground-based tracking provides poor accuracy in debris orbit propagation.

$$t_b = \frac{41.5mv}{S^2} \tag{5-3}$$

where m is the projectile mass in g, v is the projectile velocity in km/s, and S is the spacing between shields in cm (Lai, Murad and McNeil 2002).

While the previous MATE study focused on trades among the efficiency and response time of the propulsion system, grappling capability, and cost, the addition of bumper shielding to the design space introduces new trades between expected lifetime and mass penalties. To illustrate these trades, orbital debris and shielding models are added to the MATE analysis of space tug. After adding six levels of shielding to the design space (Table 5-4), several computations are performed. First, the probability of a debris collision occurring to a space tug is computed. This depends not only on debris flux and collisions per area per year but also on the satellite cross-sectional area (which varies by design). A ten-year operational life for space tugs is assumed, as is an 800 km apogee operational orbit (*i.e.*, the most-heavily utilized LEO regime with the largest number of potential on-orbit servicing customers) (UCS 2006). Second, a distribution of momentum for the impacting debris is computed, assuming an average collision velocity of 7 km/s and a probability density function of debris mass based on the integrated flux distribution (based on NASA's ORDEM2000 model[31]) and utilizing empirical relationships for relating debris diameter to debris area and debris area to debris mass (Badhwar and Anz-Meador 1989). Third, the conditional probability of surviving a debris impact is computed using the shielding model. For this purpose, survival is defined as no penetration of the primary shield. Fourth, the added dry mass for shielding is incorporated into cost, vehicle sizing, and propulsion models. The full-factorial sampling of the design variables allows for all first-order and interaction effects to be taken into account.

Table 5-4. Space Tug Design Options (n=768)

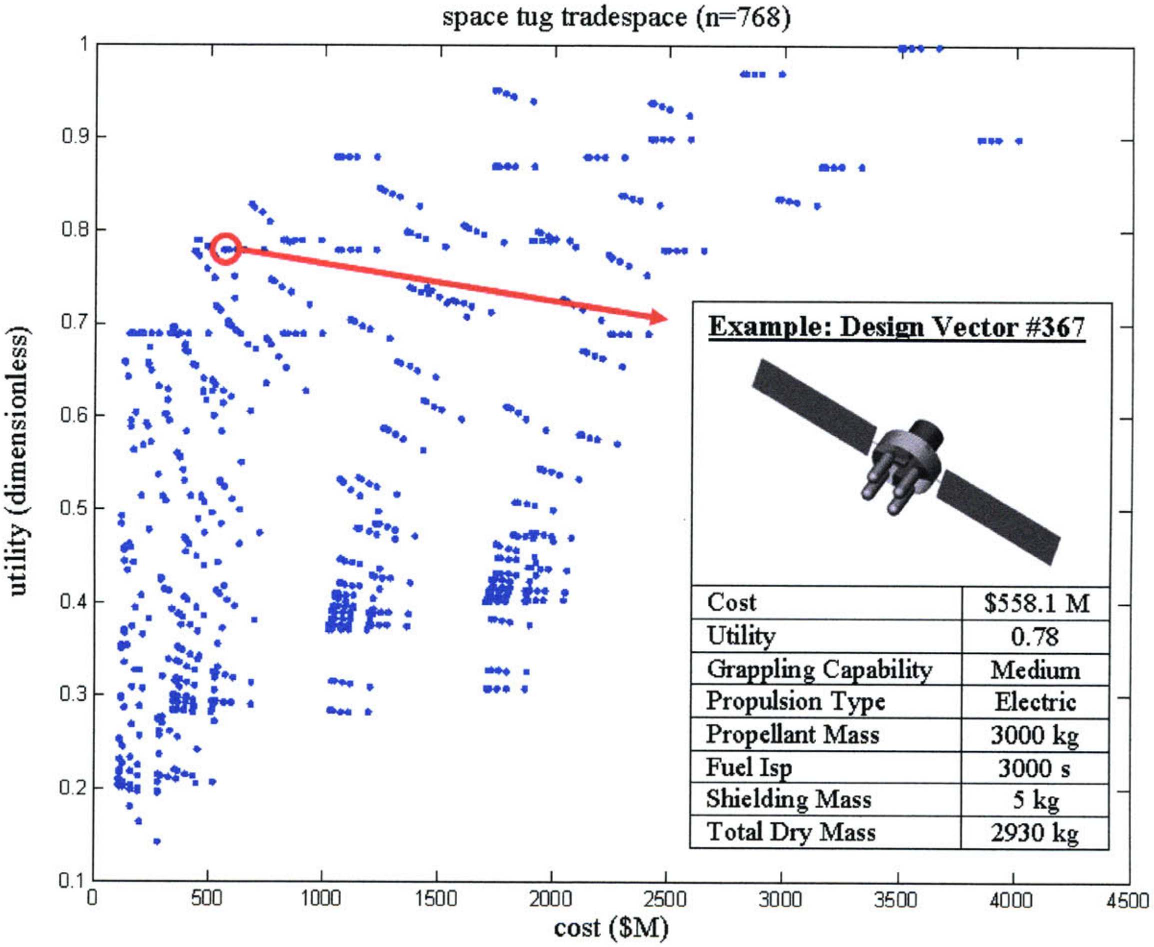
Manipulator Mass	Propulsion Type	Fuel Load (kg)	Shield Mass (kg)
Low (300 kg)	Storable bi-prop	30	5
Medium (1000 kg)	Cryogenic bi-prop	100	20
High (3000 kg)	Electric	300	100
Extreme (5000 kg)	Nuclear-thermal	600	300
		1200	500
		3000	1000
		10000	
		30000	

5.2.3. Tradespace Analysis

This section presents the results of the space tug MATE analysis. After showing the impact of bumper shielding on the baseline tradespace (where shielding only hurts performance because utility is based solely on grappling capability, ΔV, and responsiveness), an experimental tradespace is presented which display cost, utility, and survivability data for each design. In this approach, survivability is evaluated in terms of an increased probability of delivering value for the entire ten-year mission design life for a given debris environment.

[31] See http://orbitaldebris.jsc.nasa.gov/model/engrmodel.html.

The original space tug analysis showed an interesting trade-off between capability, cost, and speed (McManus and Schuman 2003). Several different classes of vehicles occupied different regions of the Pareto front, including small chemically fueled vehicles for low ΔV maneuver, servicing, and inspection; small electric vehicles that can apply considerable ΔV, although slowly; and large, expensive vehicles that can apply large ΔV's quickly but only at high launch costs (for chemical fuel) or high development cost and risk (for nuclear-thermal vehicles).



Example: Design Vector #367

Cost	$558.1 M
Utility	0.78
Grappling Capability	Medium
Propulsion Type	Electric
Propellant Mass	3000 kg
Fuel Isp	3000 s
Shielding Mass	5 kg
Total Dry Mass	2930 kg

Figure 5-6. Baseline MATE Tradespace

The current analysis adds shielding mass as a design parameter. Figure 5-6 depicts the baseline space tug tradespace. The horizontal axis is cost (in millions of dollars) and the vertical axis is multi-attribute utility, which is a function of ΔV capability, grappling system capability, and response time. Each point is a candidate system design—a unique combination of the four design variables (Table 5-4). The Pareto-efficient region of the tradespace—where utility is highest for a given expenditure—is located along the non-dominated surface running from the bottom-left through the top-left and ending at the top right region of the plot. Design #367, an "Electric Cruiser," is shown in Figure 5-6 as a sample design near the Pareto front. The diagram of the electric cruiser is from a deeper integrated concurrent engineering study reported in Galabova et al. (2003).

In the baseline MATE tradespace, utility is affected negatively by the addition of shielding, which only adds cost and reduces ΔV capability. This effect is uneven, with smaller, less expensive vehicles being affected the most. Families of vehicles differentiated only by how much shielding they have are visible as clusters. On the far left of the figure, many clusters run to the right (added costs) and also sharply down (decreased utility), indicating that adding shielding moderately increases cost, but strongly degrades utility. Other families of vehicles (*e.g.*, those near the center) show cost increases but without strong impact on utility. Finally, a few families (mostly near the top of the figure) show only cost increases, because these electric propulsion vehicles have excess ΔV capacity above user needs, so the added weight of the shielding does not decrease utility.

The baseline cost-utility tradespace is valuable to decision-makers during front-end design as it enables cost-benefit analysis across 768 concepts—avoiding the limits of local point solutions—and, most fundamentally, maps the decision-maker preference structure to the design space. However, the tradespace dimensions are of limited applicability to a survivability analysis of a space tug. The shielding design variable is shown to only add cost and/or reduce utility in this representation, meaning that every perturbation off of one of the baseline 128 designs (*i.e.*, full-factorial of first three design variables in Table 5-4) is dominated. Given that survivability features may add value to the space tug in the presence of disturbances—and given the problems associated with incorporating "-ilities" such as survivability as an attribute within multi-attribute utility functions—additional axes for survivability metrics must be added to the tradespace for a decision-maker to have an integrated perspective of cost, performance, and survivability.

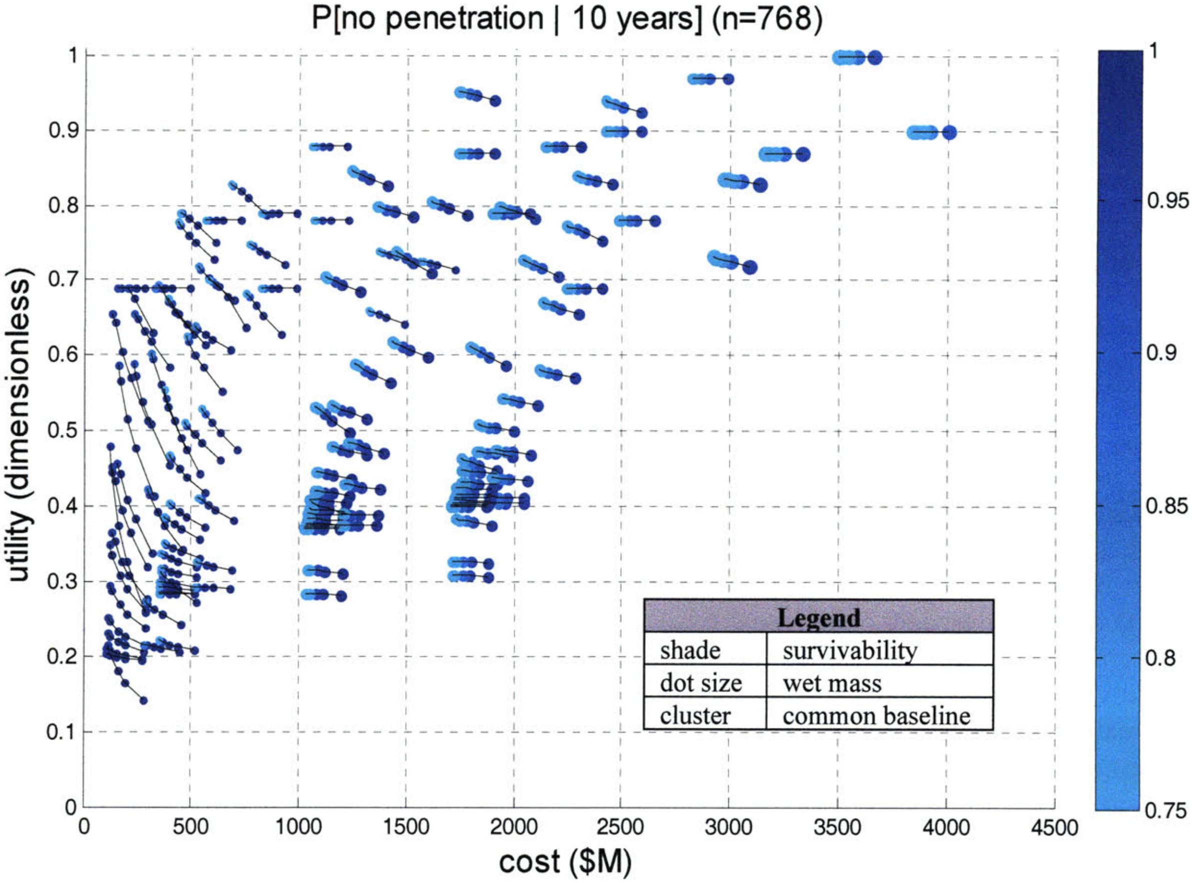


Figure 5-7. Static MATE Tradespace with Five Degrees of Freedom

Figure 5-7 provides an experimental survivability tradespace representation featuring five dimensions of data. Each design is characterized by location, shade, size and cluster. As in Figure 5-6, location specifies cost and utility. Shade specifies the probability of no bumper shielding penetration by orbital debris over the ten-year mission life. Size is proportional to the mass of the space tug and each linked cluster identifies a group of homogeneous space tugs which vary only by different levels of shielding. The impact of shielding on the cost, utility, and survivability of each baseline space tug design (n=128 before the six levels of shielding are introduced as a factor) may be directly observed. As increasing levels of shielding are added within a given cluster, cost increases, design utility decreases (usually), and the probability of sustaining mission for ten years increases. Without violating any axioms in utility theory or hiding/abstracting information from decision-makers, explicit tradeoffs may be made between the mission performance and survivability of candidate designs.

The metric for survivability in Figure 5-7 is the probability that debris does not penetrate the space tug shield over the ten-year mission life. This probability is computed by (1) estimating an effective bumper shield thickness from the shield mass in the design vector and the geometry of the design; (2), calculate the maximum size particle that the shield can withstand, and (3) using the debris distribution information and the geometry of the vehicle to calculate the probability of an impact with a particle of greater size, which is assumed to destroy the vehicle.

The results showed (not surprisingly) that small vehicles had low risk even with minimal shielding, while larger vehicles had some risk that was improved by adding shielding mass. Figure 5-7 illustrates the varying impact of shielding in different regions of the tradespace. High-cost, high-mass designs (towards the right on the chart, and represented by larger dots) clearly become more survivable as shielding is added (shown by the darkening of the dots). These improvements are obtained with a modest and consistent increase in cost (basically, the cost to build and launch the shield structure), and a modest, or in many cases zero, loss of design utility. Improvements in survivability are less pronounced for lower-cost, lower-mass designs (shade darkens only slightly, often in the first increment of shielding). For these low-mass space tugs, the added dry mass has a severe negative effect on utility as ΔV capability drops. The implication here is that there is a reduced benefit for smaller space tug vehicles to shield, at least beyond a minimal level, and there is a high cost. This makes intuitive sense as small, low-cost space tugs will have a smaller exposed cross-sectional area (reducing probability of collision) and will also incur proportionately larger ΔV penalties for shielding mass. For these lower-cost assets, survivability might be better addressed with a portfolio approach to risk management. Given ongoing debates on the value of an operationally responsive space paradigm (Section 8.3.6), these tradespaces may serve as a construct for evaluating expensive, high-capability spacecraft and lower-cost, low-capability, distributed space systems.

By making tradeoffs between cost, performance, and survivability explicit, the multi-dimensional tradespaces introduced in this section provide a framework for exploring a large set of alternative space tug architectures. While judgments of value are inherently subjective and left to decision-makers, application of MATE will enhance the discovery of these "best" designs. This approach shows that the consideration of survivability may drive the choice of "best" designs to be different from selecting Pareto-optimal designs since these solutions are generally less survivable.

5.2.4. Key Insights

Adding survivability to the trade study of space tug vehicles exposed many strengths and weaknesses of the static MATE methodology. At the outset, it was found that survivability does not fit the definition of an independent system attribute (since survivability reflects the ability to maintain performance across the attributes with time and conditions); thus, survivability cannot be combined with other attributes into a multi-attribute utility function or other single selection criteria. Perhaps, more importantly, is the knowledge of the tradespace generated by the method and presented to a decision-maker. In the test case, the knowledge of where to apply passive hardening (*e.g.*, not to small vehicles) and the modest pay-off of passive methods even for large vehicles was illustrated rapidly. The complex trade-offs involved are still difficult to visualize, but by using various graphical methods and looking for root causes for observed trends, the knowledge necessary for reasonable upfront decisions can be gained. This clarification of, and extraction of knowledge from, the analyzed tradespace is the essence of tradespace exploration, so in this sense the test case was a successful illustration of MATE.

Revisiting the set of five desirable criteria for the survivability test cases shows mixed results for the static MATE computer experiment. First, it is shown that the baseline cost-utility tradespace may be readily extended to incorporate survivability as an active trade in the decision-making process. This is an improvement from the cost-exchange ratios which do not allow such integrated trades. Unfortunately, no improvements are made *vis-à-vis* cost-exchange ratios on the second and third criteria. The lifecycle dynamics of survivability are not internalized as a fixed probability value is used to summarize survivability performance over the entire operational life. Path-dependent system vulnerability is also not considered given the assumption of binary system states. Fourth, the MATE methodology is amenable to the evaluation of systems at the architecture level. However, only satellite-level trades are demonstrated in this test case. Fifth, the use of multi-attribute utility succeeds in providing a value-centric assessment.

In summary, the second test case demonstrated that existing probabilistic conceptualizations of survivability may be readily incorporated into the static MATE methodology. However, the unsatisfied criteria (of incorporating lifecycle dynamics and internalizing path dependencies) inform opportunities to extend and customize the MATE approach for improved survivability assessments.

5.3. Test Case #3: MATE for Survivability

The third test case for examining how survivability can be quantified and used as a decision metric in tradespace studies builds directly on the second test case. Recognizing that the existing survivability metrics (*e.g.*, probability of shield penetration) and tradespace methodologies (*e.g.*, static MATE) fail to assess survivability as a dynamic, continuous, and path-dependent system property, the new survivability metrics of time-weighted average utility loss and threshold availability are operationalized in a dynamic MATE study. As introduced in Chapter 3, the metrics are based on a characterization of survivability as the ability of a system to meet required levels of value delivery during nominal and perturbed environmental conditions. To illustrate how time-weighted average utility loss and threshold availability might be utilized in trade study, the space tug tradespace is revisited and expanded to include susceptibility reduction, vulnerability reduction, and resilience enhancement features. In particular, integrated cost, performance, and survivability trades are performed for space tug vehicles incorporating bumper shielding (Lai, Murad and McNeil 2002), collision avoidance (Klinkrad 2006), and on-orbit servicing (Long, Richards and Hastings 2007) to mitigate the impact of orbital debris.

The modeling approach for applying the survivability metrics consists of four aspects: (1) static Multi-Attribute Tradespace Exploration, (2) Epoch-Era analysis (Ross and Rhodes 2008), (3) stochastic simulation of space tug operation, and (4) Monte Carlo analysis. First, the legacy MATE study on space tug vehicles is extended to incorporate a broader set of survivability enhancement features. Second, Epoch-Era Analysis is performed in which satellite lifetimes (*i.e.*, eras) are modeled as sets of discrete time periods with fixed contexts and needs (*i.e.*, epochs). Applying techniques from network analysis, static tradespaces from MATE are linked *over time* wherein nodes represent satellite configurations and arcs represent satellite state transitions. System eras for the candidate space tug designs are modeled by stringing together representative sequences of baseline (*i.e.*, ambient environment) and disturbance epochs (*i.e.*, debris conjunction events).[32] Third, a stochastic simulation of space tug operations is performed

[32] Given the focus on survivability in this paper, the only changes across Epoch boundaries in the space tug model are finite-duration disturbance events in the environment (*i.e.*, debris impacts) and changing stakeholder expectations (*i.e.*, short-term relaxation of stakeholder expectations during disturbance and recovery Epochs). When

in which debris impacts are modeled as forced transitions of space tugs in the tradespace to lower utility designs (or end-of-life states). Each run of the simulation produces a utility trajectory (*i.e.*, a plot of multi-attribute utility over time) for a candidate space tug in the tradespace. Fourth, a Monte Carlo analysis is performed across the stochastic, path-dependent utility trajectories, and the survivability metrics are applied.

This section follows the general format of the previous two test cases. Following a description of how active survivability strategies are incorporated into the design vector, the software architecture of the dynamic space tug model is summarized and survivability metrics (including both existing and new) are applied to a series of experimental tradespaces. Local response surfaces are drawn to illustrate the impact of the survivability features in each region of the tradespace. After demonstrating the ability of the metrics to discriminate among the varying survivability of design alternatives and how to incorporate the metrics into traditional cost-utility tradespaces, key insights of the test case are discussed.

5.3.1. Addition of Active Survivability to Space Tug Design Vector

Building on both the baseline space tug trade study and second test case that investigated only passive bumper shielding, the dynamic MATE model presented in this section incorporates passive and active survivability strategies into the tradespace.

Table 5-5. Space Tug Design Options (n=2560)

Design Variables

Manipulator Mass	Propulsion Type	Fuel Load (kg)	Shield Mass (kg)	Servicing	Collision Avoidance
Low (300kg)	Storable bi-prop	30	30	no	no
Medium (1000kg)	Cryogenic bi-prop	100	100	yes	yes
High (3000 kg)	Electric (NSTAR)	300	300		
Extreme (5000 kg)	Nuclear Thermal	600	500		
		1200	1000		
		3000			
		10000			
		30000			

survivability features

While the baseline MATE study focused on trades among the efficiency and response time of the propulsion system, grappling capability, and cost, the addition of survivability features to the design space introduces new trades between cost, design utility (*i.e.*, utility achieved under nominal conditions at beginning-of-life), and survivability. Table 5-5 depicts the six design variables used to specify a given design vector (*i.e.*, design alternative), including three variables for survivability features. Each of the three variables is intended to drive a particular type of survivability. For Type I survivability, susceptibility reduction is achieved through active collision avoidance of cataloged debris objects. Susceptibility is also reduced by selecting design vectors of small spacecraft (which will have smaller exposed cross-sectional areas to the debris flux). For Type II survivability, vulnerability is reduced by selecting higher levels of bumper shielding. In addition, vulnerability may also be reduced by selecting space tugs of higher capability—potentially providing margin to degradation losses. For Type III

focused on survivability, transitions in a dynamic MATE study primarily comprise (1) forced transitions to lower utility states during disturbance events and (2) transitions to higher utility states during recovery.

survivability, resilience may be enhanced by paying an upfront insurance fee for on-orbit servicing and repair in the event of non-catastrophic debris impacts.

5.3.2. Implementation of Dynamic Model

Figure 5-8 provides a high-level perspective of how the space tug survivability model is implemented over seven general steps. First, 2560 space tugs designs are defined through a full-factorial sampling of the six enumerated design variables.

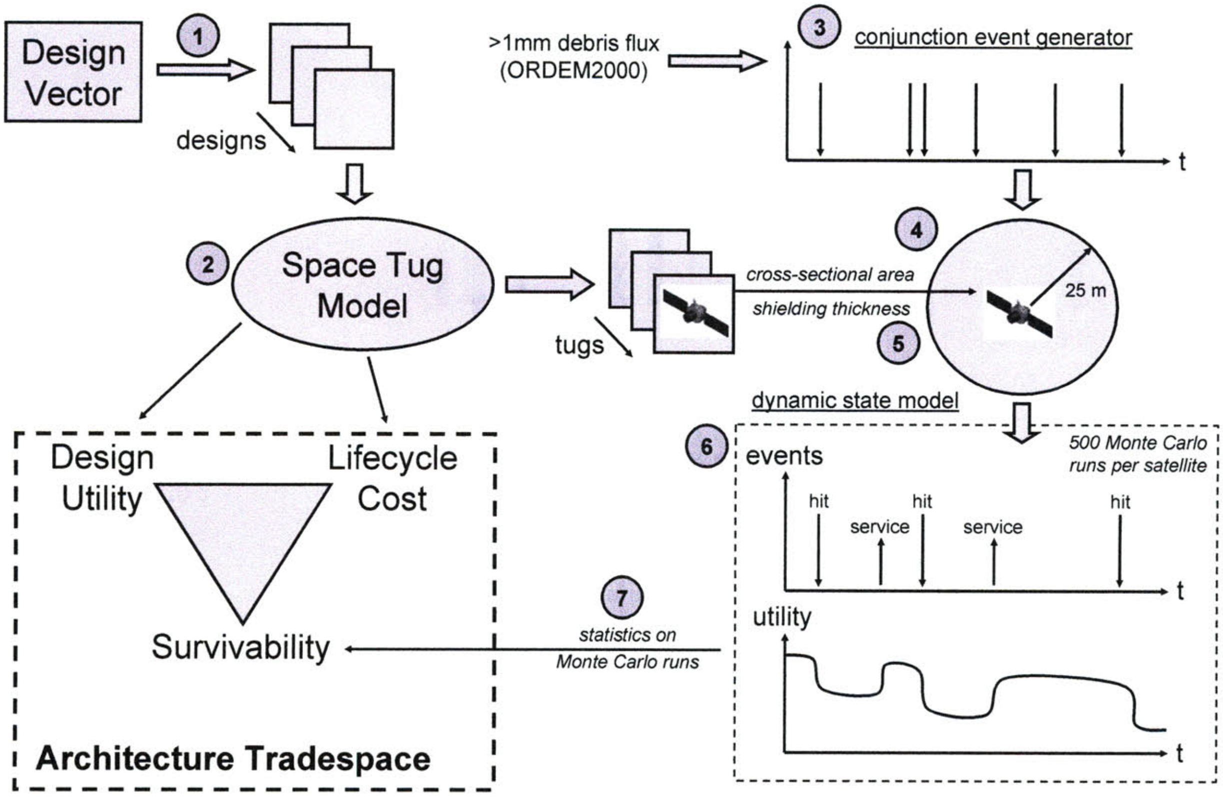


Figure 5-8. Overview of Dynamic Space Tug Model

Second, the static space tug model and multi-attribute utility function are used to assess the lifecycle cost and design utility of each design vector. After imposing dry mass and cost penalties for the shielding (variable mass penalty as specified by design variable), servicing ($100 million dollar insurance fee and 50 kg docking ring) (McVey 2002), and warning service for active collision avoidance (assumed fee of 5% of baseline space tug cost), the legacy model calculates the lifecycle cost and design utility of the expanded design vector.

Third, conjunction events—defined here as the passage of debris object greater than 1 mm in diameter within 25 meters of the satellite—are generated according to a Poisson process where the arrival rate is determined by the debris flux. Assuming that the space tugs are launched in 2009 to a 800 km circular orbit at a 42.6° inclination (a relatively populated region of LEO), the orbital debris flux is extracted from NASA's ORDEM2000 model. Flux is assumed isotropic and constant over the ten-year operational life.

Fourth, given a conjunction event, the baseline susceptibility of each satellite to a debris hit is computed as the ratio of the satellite cross-sectional area to the cross-sectional area of the conjunction sphere. Figure 5-9 shows a histogram of the probability of a hit given a conjunction event for all candidate space tug designs.

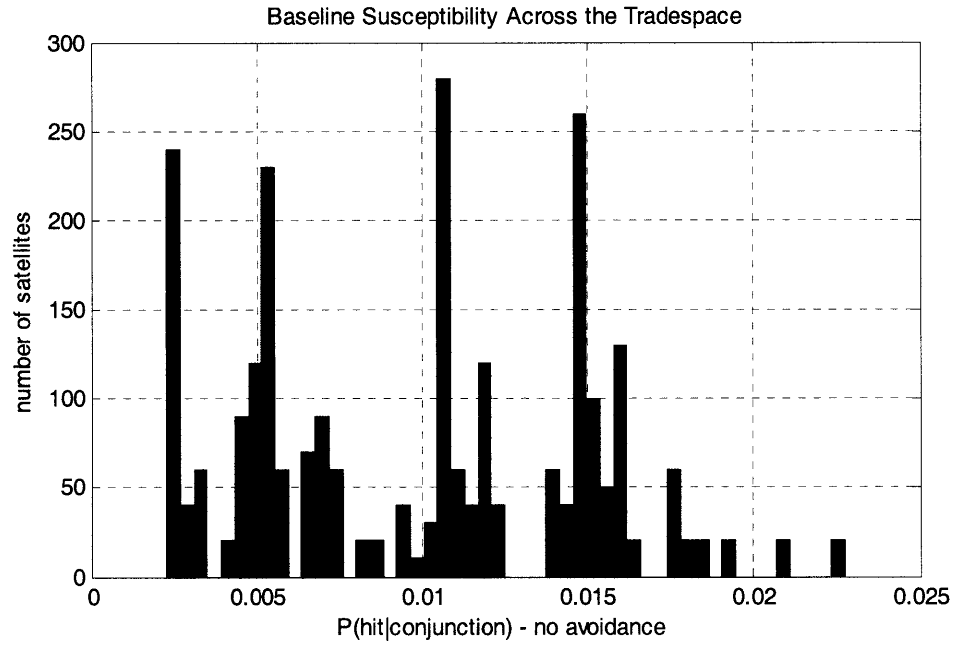


Figure 5-9. Conjunction Outcomes

Fifth, given a hit, the probability of an encounter with one of three possible sizes of debris is computed: (1) a small debris impact, (2) a medium debris impact, or (3) a large debris impact. (Debris of <1mm diameter are termed micro and are assumed to have no impact on system functionality.) Table 5-6 enumerates the impact outcomes as reported in Remo (2005) as well as the modeling assumptions made regarding the degradation of a space tug design for a given size impact. The modeling of damage due to impact is a complex subject depending both on the debris and the spacecraft being impacted. As this is a conceptual design study with limited characterizations of the debris and spacecraft, the damage assumptions are coarse. The energies involved in large debris impacts (>10 cm) are so great that it is unlikely that any spacecraft would survive (Hastings and Garrett 1996). Conversely, when encountering debris smaller than 1mm, spacecraft without dedicated shielding experience limited degradation. For modeling simplicity, these micro impacts are not considered. The effect of medium impacts will depend on which part of the spacecraft is hit. Regardless of where the impact occurs, some spacecraft capability will be lost. Since spacecraft behavior is modeled in terms of capability, the effect of impact is represented as a reduction in space tug capability level.

Table 5-6. 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

While the probability of encounters with micro and large debris objects are constant for a given exposed cross-sectional area, the probability of encounters with small and medium debris objects varies relative to the maximum debris size impact that can be sustained by the bumper shielding of a given space tug without deflection, rupture, or spalling. (As discussed in detail in Section 5.2.2, the size of objects large enough to penetrate the bumper shield varies based upon the thickness of the shield, which in turn depends on the shield mass and satellite body area. Using an empirically-derived bumper shield model, empirically-derived relationships for relating debris diameter to debris mass, and assuming the approximate average orbital relative velocity in ORDEM2000 of 7 km/s, the maximum debris diameter for a small hit is computed.) Table 5-6 illustrates this variable threshold as x cm, meaning that an impact by a debris particle <x cm will not penetrate the shield. However, assuming that the shield covers the leading edge ±45° and surfaces 90° to the ram direction, there is an approximately 10% chance that impact occurs on an unshielded portion of the spacecraft (Wertz and Larson 1999). Therefore, hits by small debris are assumed to penetrate the spacecraft 10% of the time, reducing the space tug capability level. Finally, given the three critical debris diameter thresholds of 1 mm, x cm, and 10 cm for each satellite, and using the spatial density of debris of those diameters in ORDEM2000 (Figure 5-10), the cumulative probability that the intercepting particle of debris falls into each of the debris size bins is computed.

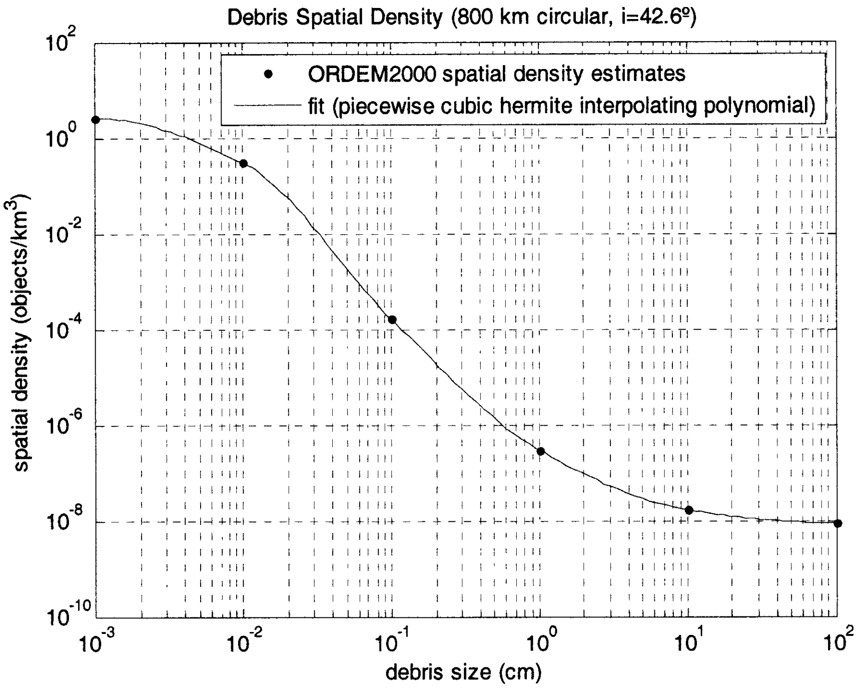


Figure 5-10. Spatial Density of Debris

Because the outcome of a conjunction event is probabilistic and path-dependent in nature, a Monte Carlo analysis is performed over the sixth step. The ten-year operational life of each space tug is simulated 500 times to generate a diverse range of possible utility trajectories.[33] While ΔV expenditures from normal mission operations slowly degrade capability (at a rate of 1/15 of the ΔV budget per year), the most significant drivers of utility change are debris impact events and servicing. For each conjunction in a given run of the simulation, the probability of an encounter with a given type of debris is used to probabilistically insert disturbance epochs of small, medium, and large debris encounters. The implications of a given encounter may be uneventful, non-catastrophic (utility degradation), or catastrophic (*U=0* for the remainder of the 10-year period). In the event of an encounter with a large debris object, space tugs that did not invest in collision avoidance are catastrophically impacted while those tugs investing in avoidance are able to maneuver away from these cataloged objects with 99% success (Klinkrad 2006). In the event of a medium encounter, the debris object is too small to track (and hence avoid) but too large to completely shield. Space tug degradation from this penetrating impact is modeled as a forced transition in the tradespace network whereby the grappling capability design variable of the space tug is reduced by one discrete level. For example, if a space tug with "low" grappling capability (U_i*=.3*) is subjected to a non-catastrophic hit, grappling capability drops to "none" (U_i*=.0*), a minimalistic operational state in which no utility is derived from grappling. For those design vectors including a servicing option, an on-orbit repair is attempted following a non-catastrophic hit. Successful servicing missions restore grappling capability to the original (baseline) level in the design vector. (A given servicing mission is assumed to have a 70% success rate. Response times are lognormally distributed with a mean of six months and a

[33] See Section 6.6.4 for a general discussion on determining the appropriate number of Monte Carlo trials in a convergence study.

standard deviation of a year.) In the event of an encounter with a small debris object, any debris hitting the bumper shield is stopped. However, as bumper shielding does not completely cover the satellite (as it is concentrated around the most susceptible and vulnerable regions), a 10% probability of non-catastrophic impact is assumed.

Having sampled 500 utility trajectories over the distribution of possible impact and recovery sequences for each of the 2560 space tug designs, summary statistics are collected in the seventh and final step of the model to measure trends in lifecycle survivability. These statistics include the existing and proposed metrics of survivability discussed in the following section.

5.3.3. Tradespace Analysis

This section presents the results of the dynamic MATE analysis. After showing the impact of the survivability features on the baseline tradespace, results from the dynamic state characterization of space tug designs are shown. These results include sample utility trajectories, application of the survivability metrics within the baseline tradespace, and the introduction of a new survivability tradespace that allows integrated trades to be made among cost, performance, and survivability. The section concludes with a response surface analysis of each survivability feature—investigating the impact of shielding, collision avoidance, and servicing on each space tug design.

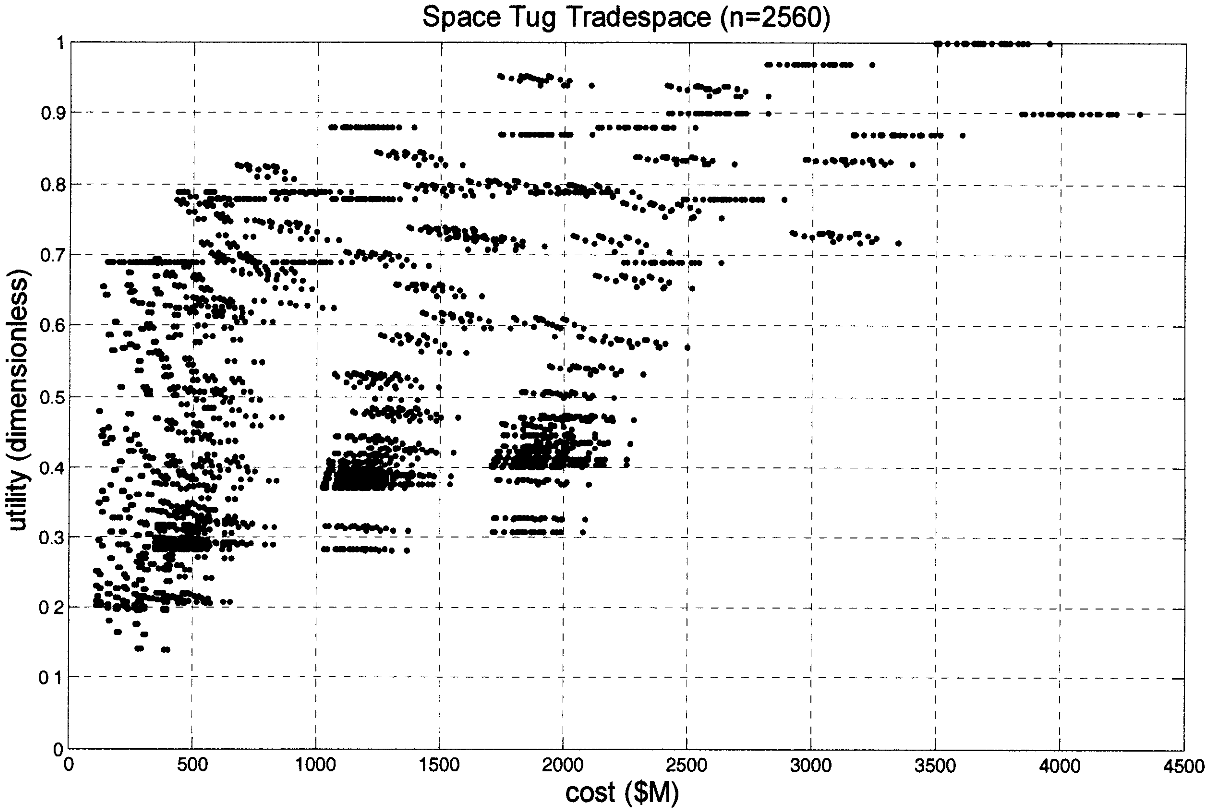


Figure 5-11. Baseline Space Tug Tradespace

While the second test case added 6 possible combinations of survivability features for each of the design alternatives in the baseline set of 128 design vectors, this test case adds 20 combinations. Figure 5-11 depicts the new space tug tradespace of 2560 design alternatives. During normal operating conditions, space tug utility is affected negatively by the addition of survivability features which only add cost and reduce ΔV capability. As discussed in the previous test case, the baseline tradespace dimensions are of limited applicability since all designs incorporating survivability are dominated solutions in this representation.

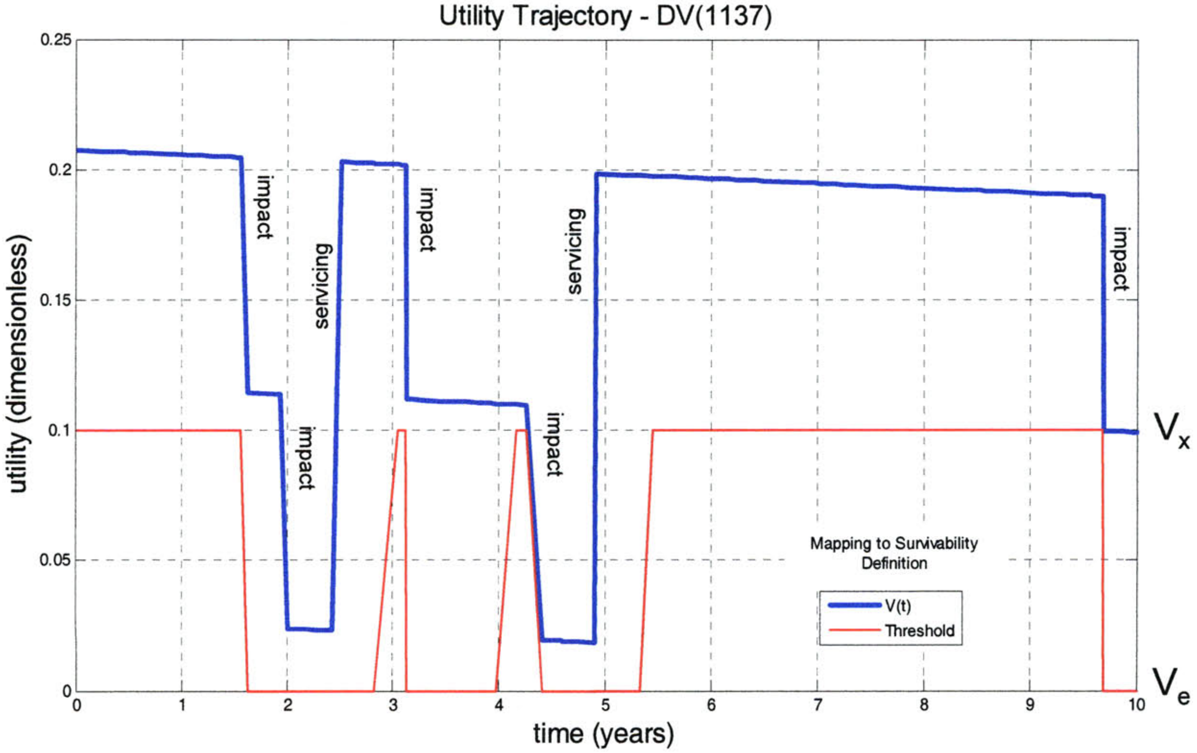


Figure 5-12. Sample Utility Trajectory

As discussed in Chapter 3, 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. The dynamic space tug model operationalizes this definition by generating utility trajectories of alternative designs in the presence of orbital debris events. Figure 5-12 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 18 months of operation (modeled as nominal ΔV expenditures), two non-catastrophic debris impacts occur in quick succession during the latter part of the second year. Due to the reduction in expectations from V_x to V_e for a year 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 events—consecutive debris hits followed by successful servicing—occurs between the third and fifth years. In both cases, large quantities of utility are lost while critical value thresholds are met.

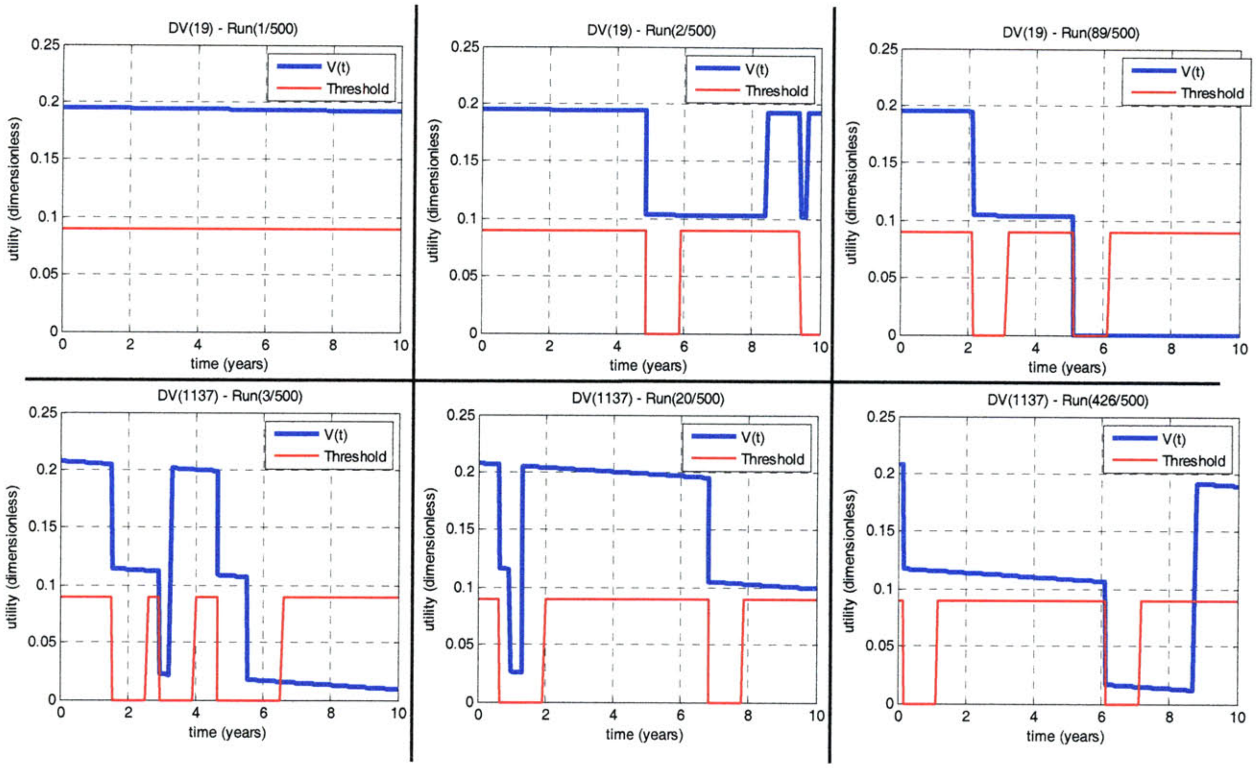


Figure 5-13. Sample Utility Trajectory Outputs from Design Vectors 19 and 1137

Figure 5-13 depicts six more sample utility trajectories. The top row illustrates the outcomes from three Monte Carlo runs of design vector 19, DV(19), and the lower row illustrates three runs of DV(1137). The cell in the upper left depicts the most common utility trajectory output from the model: slight utility degradation over time without any debris impacts. While the middle upper cell shows DV(19) receiving (and recovering from) two non-catastrophic debris impacts, the upper right cell shows the mission ending prematurely at year five from a catastrophic impact. Similar erratic utility trajectories are observed across the lower row. Interestingly, while both run 3 (bottom left) and run 426 (bottom right) of DV(1137) reveal an active space tug at end-of-life, both spend at least a year below V_x due to failed and delayed servicing operations, respectively.

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 (*e.g.*, illustrated by rows in Figure 5-13). 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 introduced in Chapter 3—*time-weighted average utility/utility loss* and *threshold availability*—are applied as aggregate measures for each set of space tug utility trajectories.

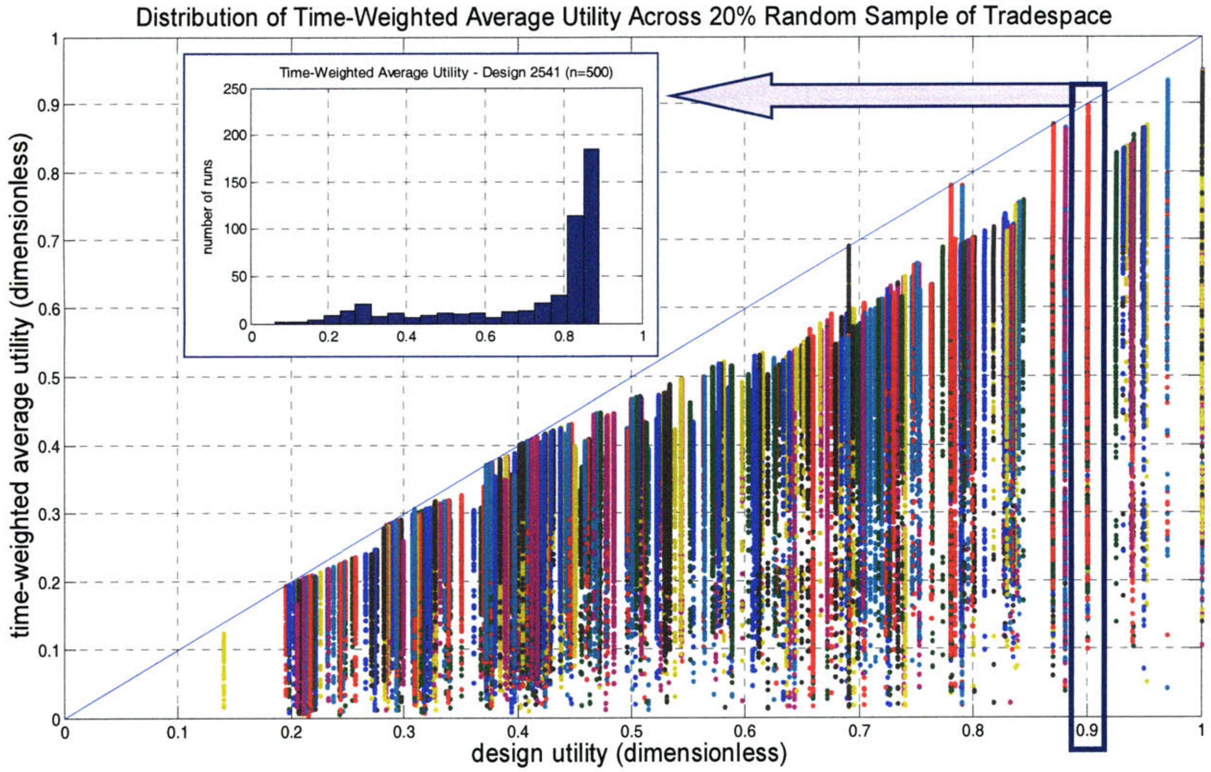


Figure 5-14. Distributions of Time-Weighted Average Utility

Figure 5-14 depicts the distributions of time-weighted average utility achieved by 20% of the design vectors over 500 Monte Carlo runs. (A random sample of 20% was selected to aid in information visualization.) Each column of identically-shaded points represents the distribution of time-weighted average utility for a single space tug design vector. To organize the data, the columns are ordered along the horizontal axis in terms of design utility—the deterministic beginning-of-life utility (V_0) achieved by a space tug before stochastic losses accrue from normal degradation and orbital debris. The design utility here is equivalent to the utility axis in the baseline tradespace (Figure 5-11). A 45° line is also drawn to show the maximum time-weighted average utility value achievable.

The results are illuminating, showing a consistent pattern of highly-skewed distributions towards design utility. The histogram of DV(2541) in Figure 5-14 is displayed as a representative distribution of the highly-skewed behavior of time-weighted average utility across simulation runs. One interesting trend observed is the general regression of maximum time-weighed average utility values from V_0 for space tugs as design utility increases. This is due to both the increased susceptibility of larger (and generally higher-utility) space tug vehicles to orbital debris and to the lower ΔV margins of the more massive space tug vehicles. (Given the full-factorial enumeration of design vectors, tradespace artifacts, such as the paring of low fuel mass with high-capability tugs, may result.) An additional behavior across the distributions is the presence of maximum time-weighted average utility outliers (in which no losses or degradation are observed *vis-à-vis* the design utility line) beginning around design utility values of 0.7. These outliers are attributed to simulation runs of high-capability electric propulsion space tug designs that were set with excessive ΔV margins and that did not suffer from orbital debris impacts.

The highly-skewed, long-tailed nature of the distributions of time-weighted average utility across simulation runs was also observed for the distributions of threshold availability. Figure 5-15 shows the output from DV(2541) utility trajectories as a sample distribution.

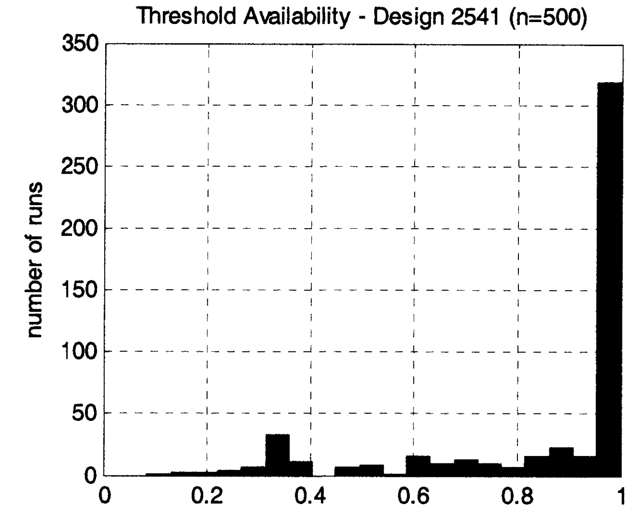


Figure 5-15. Sample Distribution of Threshold Availability

Having generated a data set of utility trajectories and having applied two new measures of lifecycle survivability, the new metrics are compared to existing survivability metrics and integrated with measures of cost and design utility.

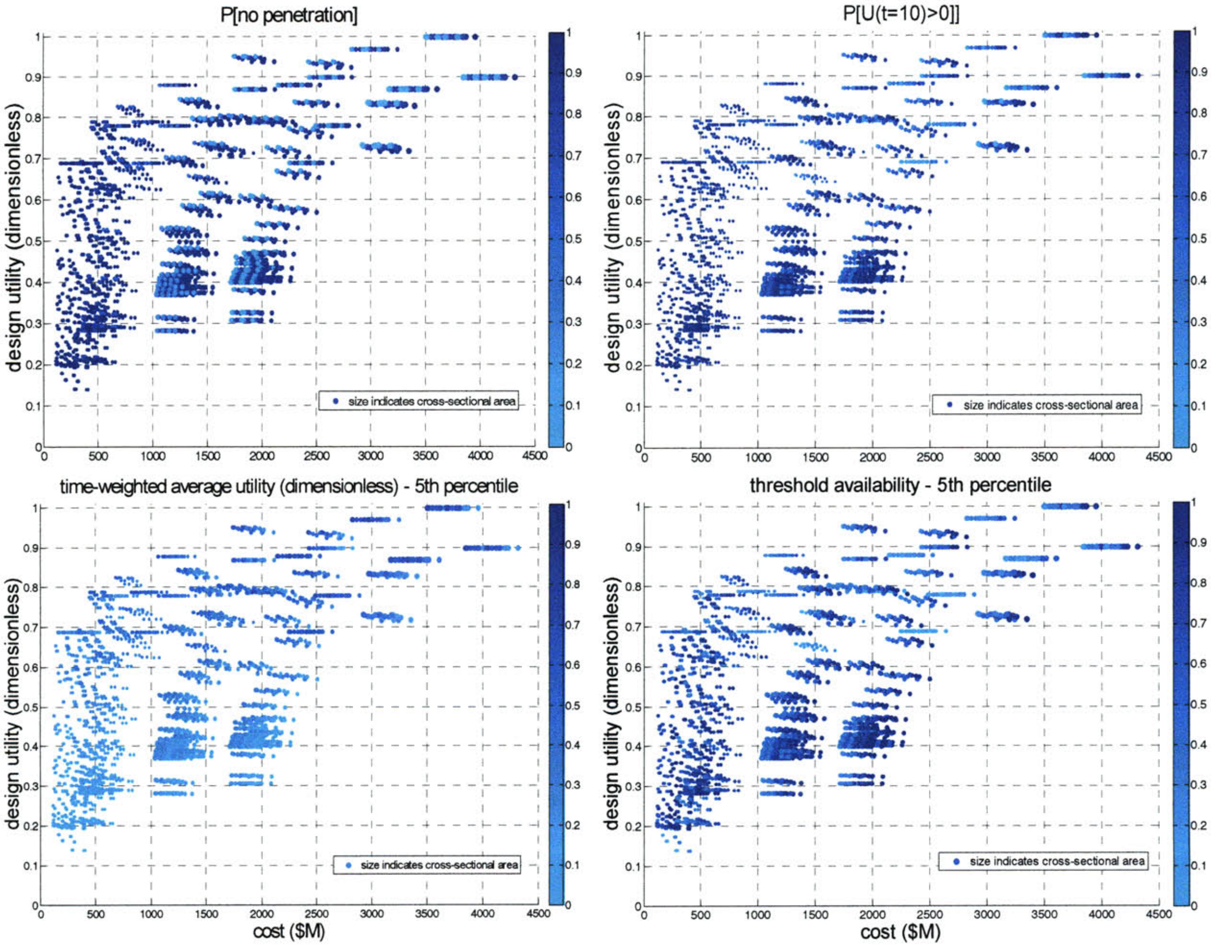


Figure 5-16. Application of Survivability Metrics to Baseline Tradespace

Figure 5-16 presents four separate survivability tradespaces, each incorporating one of four different survivability metrics to the baseline cost-utility tradespace in Figure 5-11. The top two tradespaces apply existing static conceptualizations of survivability while the bottom two tradespaces apply the proposed dynamic measures of survivability. Each survivability metric is depicted in shade (*i.e.*, darker means more survivable). In addition, to indicate the varying susceptibility of small and large space tugs to orbital debris, the size of each point in the tradespaces is correlated with exposed cross-sectional area.

The results across the four tradespaces vary tremendously, indicating the importance of understanding and selecting the correct metric or metrics for evaluating system survivability (*i.e.*, depending on the metric chosen, very different conclusions may be drawn). The top-left tradespace, P[no penetration], shades each space tug design by the probability of no debris penetration over the 10-year operational life. In this representation, lower-cost designs achieve a high degree of survivability due to their low-susceptibility while the survivability of high-cost designs fluctuates as a function of shielding and collision avoidance. (Resilience enhancement strategies, such as servicing, are exogenous to this survivability metric.) The top-right tradespace, P[U(t=10)>0], is shaded by the probability of a non-zero utility (*i.e.*, operational) space tug at end-of-life. Here, the high survivability of lower-cost designs is again observed.

The survivability of high cost designs varies considerably as a function of all three survivability features.

The bottom-left tradespace in Figure 5-16, time-weighted average utility–5th percentile, shades each point by the level of time-weighted average utility achieved by 95% of the simulation runs of that design vector. For example, a value of 0.53 for time-weighted average utility–5th percentile means that 95% of the simulation runs of that design vector achieved a time-weighted average utility of at least 0.53. (Rather than use a potentially misleading measure of central tendency such as average for the highly-skewed distributions, aggregate simulation results for time-weighted average utility and threshold availability are reported as percentiles.) The results here are naturally correlated with design utility. Many designs deemed survivable by this metric are found in the interior of the traditional cost-utility Pareto front. Interestingly, clusters of space tugs (varying only by survivability design variables) are observed where there is a non-monotonic relationship between adding levels of survivability features (indicated by rising costs) and time-weighted average utility. The bottom-right tradespace, threshold availability–5th percentile, shades each point by the proportion of time over the 10-year operational life spent above the critical value threshold. (As illustrated in Figure 5-13 and discussed in Chapter 3, this threshold varies depending on environmental context.) In contrast to time-weighted average utility, threshold availability generally rises as survivability features are added to each space tug. Threshold availability also appears to be sensitive to space tug size as smaller, less-susceptible designs achieve higher availability than their larger counterparts. Exceptions to these trends are also observed, including the low-availability of the extremely low-cost designs due to their tight performance margins.

The four tradespaces shown in Figure 5-16 present four conflicting (yet interdependent) perspectives regarding the survivability of the 2560 candidate space tug designs. Each tradespace presents useful information to the decision-maker. However, there is a need to aggregate the information to allow integrated tradeoffs among other decision metrics for cost, performance, schedule, and risk. While the upper two tradespaces communicate the relative survivability of designs based on binary calculations of survivability, the two lower tradespaces are based upon the definition of survivability as a continuous, stochastic, and path-dependent property that is assessed over the entire operational life. Therefore, in order to incorporate all of the information contained in the utility trajectories (rather than small samples of the data such as the utility state at end-of-life), the next two tradespaces focus on applying the new survivability metrics.

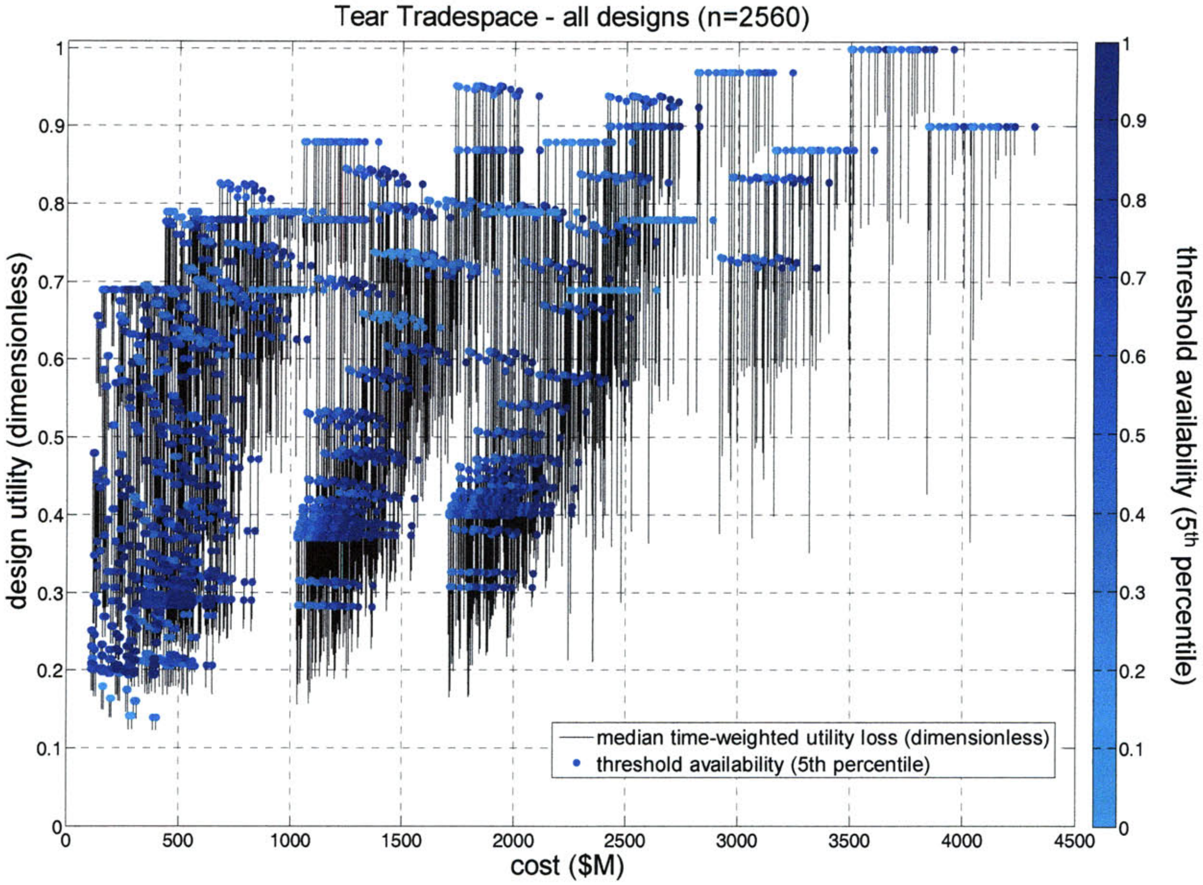


Figure 5-17. Survivability "Tear" Tradespace – Space Tug

To address the need for trading lifecycle cost, performance, and survivability of design alternatives, Figure 5-17 introduces a survivability "tear(drop)" tradespace representation. (Use of the word "tear" is meant to describe regret associated with system utility loss.) The purpose of the survivability tear tradespace is to integrate deterministic cost and design utility data with the distributions of time-weighted average utility loss and threshold availability. Preserving the cost and design utility axes of the baseline tradespace, the new survivability metrics are integrated using shade (threshold availability–5th percentile) and a line drawn to the median time-weighted average utility. By definition (see Section 3.3.2), the length of this line is the median time-weighted utility loss across the 500 utility trajectories for each space tug design. Rather than the 95th percentile, the median is selected for summarizing the distribution of time-weighted utility loss for two reasons: (1) ease of visualization for this particular data set by shortening the length of utility loss tails (from 95th to 50th percentile) and (2) recognition that decision-makers are likely to be more risk-averse regarding threshold availability (a construct for measuring assured access to some level of minimum capability) than time-weighted average utility (a construct for assessing degree of degradation).

Some interesting trends can be observed in Figure 5-17, such as the poor performance of very low-cost and very expensive designs in terms of threshold availability (due to low-performance margins and high-susceptibility, respectively). Irregular reductions in utility loss can be observed as survivability features are added to clusters of baseline space tug designs. Smaller utility losses appear to occur in the lower-cost (smaller), lower-susceptibility region of the tradespace. Unfortunately, one consequence of tagging each of the 2560 design alternatives with four data attributes is that Figure 5-17 becomes very concentrated and difficult to interpret.

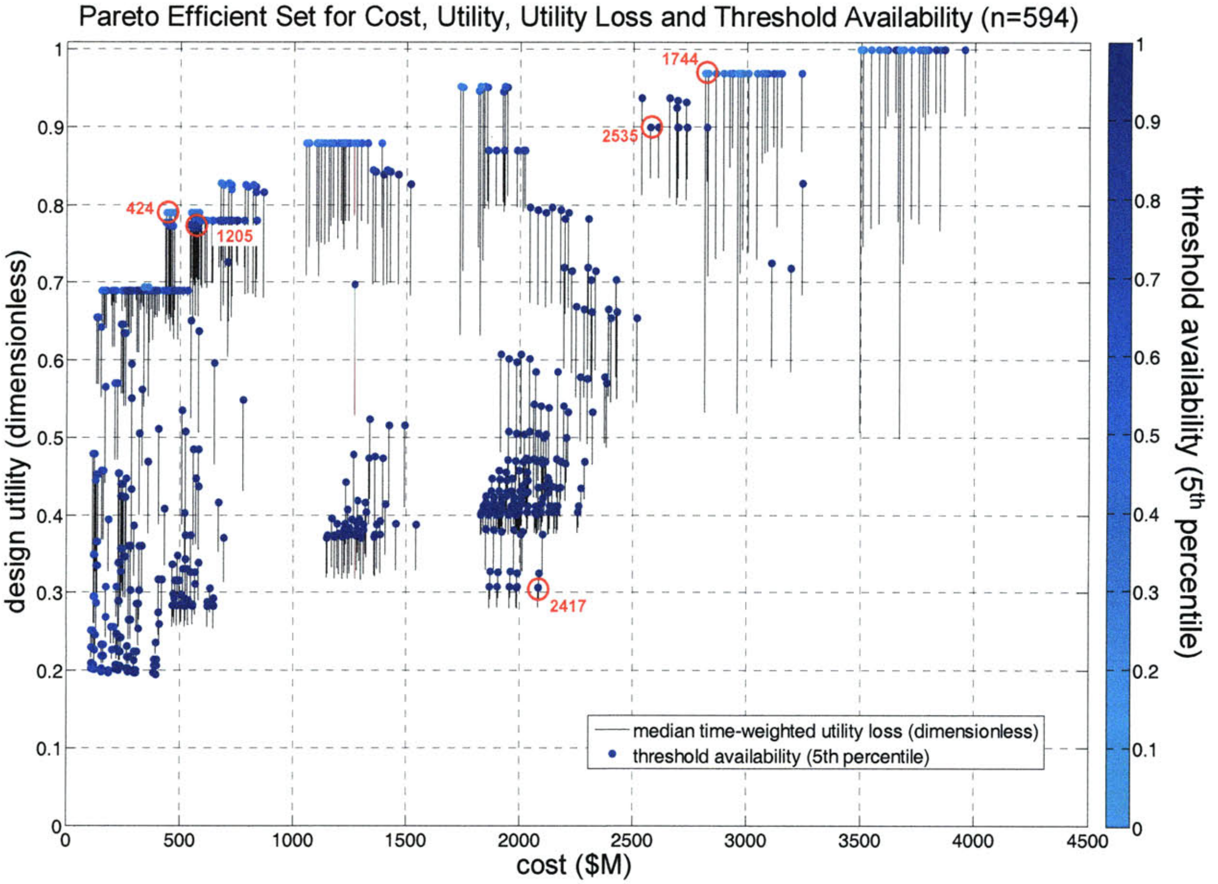


Figure 5-18. Four-Dimensional Pareto Surface of Survivability Tear Tradespace

Figure 5-18 reduces the concentration of Figure 5-17 by filtering the 2560 designs for Pareto-optimality over the four decision metrics: cost, design utility, median time-weighted utility loss, and threshold availability. When considering the tradespace in four dimensions, the surface of Pareto efficient designs contains three individual Pareto sets (as determined by a projection onto the cost-utility, cost-availability, cost-utility loss planes) as well as other points that would not project onto any of these two-dimensional surfaces. These other points exist at the tradeoffs among design utility, threshold availability, and time-weighted utility loss for the decision-maker and represent "compromise" value solutions.

Counterintuitively, as decision metric axes are added to filter for Pareto-efficiency, more designs will remain after filtering in the survivability "tear" tradespace. This is because as each axis is added, a new two-dimensional Pareto front is created with a new set of projected compromise solutions. For example, a cost-utility filter applied to Figure 5-17 leads to 111 Pareto-efficient designs while a cost-utility-utility loss filter leads to 279 Pareto-efficient designs. As a fourth metric is added for filtering (as in Figure 5-18), 594 designs are deemed Pareto-efficient. This growth of Pareto-efficient designs as decision metrics are added is analogous to the multi-stakeholder problem in utility theory (Keeney and Raiffa 1993).

One implication of filtering over the four decision metrics is that several interior designs become Pareto-efficient based upon their superior performance in terms of survivability. Rather than only allowing the selection of designs dominant in terms of cost and utility at beginning-of-life, the filtered survivability tear tradespace presents alternative designs that may offer superior performance over a lifecycle of disturbances.

Having filtered the tradespace, it is now possible to conduct trades among designs along the four-dimensional Pareto surface. For example, Table 5-7 lists the design variable settings and performance parameters for five design vectors circled in Figure 5-18. In the $400-600M range, the nuclear DV(424) is optimized in terms of cost and design utility while the electric DV(1205) is slightly dominated in terms of cost and design utility but with a 68% improvement in 5th-percentile threshold availability. As an example in the $2.5-3B range, DV(1744) is similar to DV(2535) in cost and design utility but requires a tremendous sacrifice in survivability (*i.e.*, 0.43 rather than 0.06 median utility loss and a 0.76 difference in threshold availability). As an extreme case of high-survivability, the characteristics of DV(2417) are also shown. As indicated in Figure 5-18, all five design are located along the four-dimensional Pareto surface.

Table 5-7. Characteristics of Circled Design Vectors in Figure 5-18

Design Vector ID	424	1205	1744	2535	2417
Manipulator Capability	Low	Medium	High	Extreme	Extreme
Propulsion System	Nuclear	Electric	Nuclear	Electric	Electric
Propellant Mass (kg)	3000	1200	30000	10000	30
Shield Mass (kg)	30	100	30	500	1000
Avoidance	Passive	Active	Passive	Passive	Active
Serviceable	No	Yes	No	Yes	Yes
Cost ($M)	439.1	577.6	2815	2607	2079
Design Utility	0.79	0.77	0.97	0.90	0.31
Median Utility Loss	0.13	0.11	0.43	0.06	0.02
Threshold Availability (5%)	0.32	1.0	0.24	1.0	1.0

The results in Figure 5-18 and Table 5-7 demonstrate two key benefits of the survivability tear tradespace analysis: screening and down-selecting among thousands of design alternatives with survivability as an explicit decision criterion. Interestingly, most of the designs in the cost-utility Pareto front have much lower threshold availability—and considerably higher utility loss—than interior designs while several of the highly-survivable space tugs are only slightly dominated in terms of cost and design utility.

Having introduced a survivability "tear" tradespace for enabling integrated trades to be made across alternative concepts in terms of cost, performance, and survivability, the impact of each of the three survivability design variables on the survivability of each of the 128 baseline designs (*i.e.*, full-factorial of first three, non-survivability design variables in Table 5-5) is now examined. This analysis may be used for maximizing the survivability of an individual satellite (if a baseline design concept has already been selected) as well as for investigating the overall sensitivity of the satellite tradespace to various survivability enhancement features.

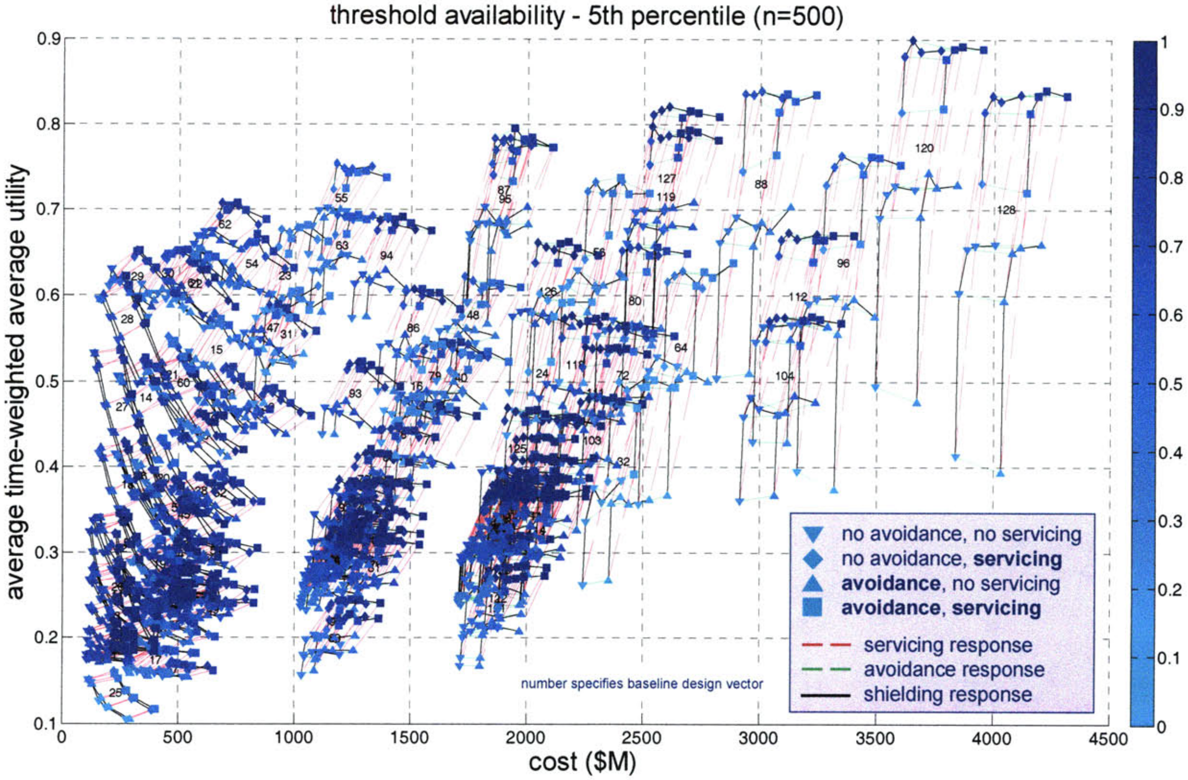


Figure 5-19. Survivability Response Surfaces – 128 Baseline Designs

Figure 5-19 plots survivability response surfaces for each of the baseline designs. Each design point is located in terms of cost and average time-weighted average utility[34] and shaded by 5th percentile threshold availability. Linked clusters (labeled 1 through 128) indicate a common baseline space tug of fixed manipulator mass, propulsion type, and fuel load. The impact of survivability features is evaluated by finding the lowest-cost inverted triangle in each cluster to identify the baseline space tug design (which incorporates only 30 kg of shielding and no avoidance or servicing). Then, the response surfaces for shielding, servicing, and avoidance may be identified by examining the solid black, dashed red, and dashed green lines, respectively. Designs incorporating no servicing are represented with three-sided shapes (*i.e.*, as triangles for designs with avoidance and as inverted triangles for designs with no avoidance) while designs that do incorporate servicing are represented as four-sided shapes (*i.e.*, as squares for designs with avoidance and as diamonds for designs with no avoidance).

[34] Time-weighted average utility is the average across a single trajectory while average time-weighted average utility is the average of this value across the set of 500 Monte Carlo trials. As the response surface plots are drawn to reveal causal relationships, average is used in place of median for reporting time-weighted average utility to accentuate variance in survivability outcomes.

Interesting trends may be indentified in the (relatively) sparse, high-cost region of Figure 5-19. For example, increasing the shielding appears to increase threshold availability as shielding mass is increased, while average utility benefits only from the initial increases in shield mass. Avoidance appears to have no statistically significant impact across the 500 runs (as availability is constant and average utility fluctuates slightly up or down). Servicing has a very positive impact on both survivability metrics in this region of the tradespace. Unfortunately, it is hard to extract survivability response surface trends across this display of the entire tradespace given the density of clusters in lower-cost regions.

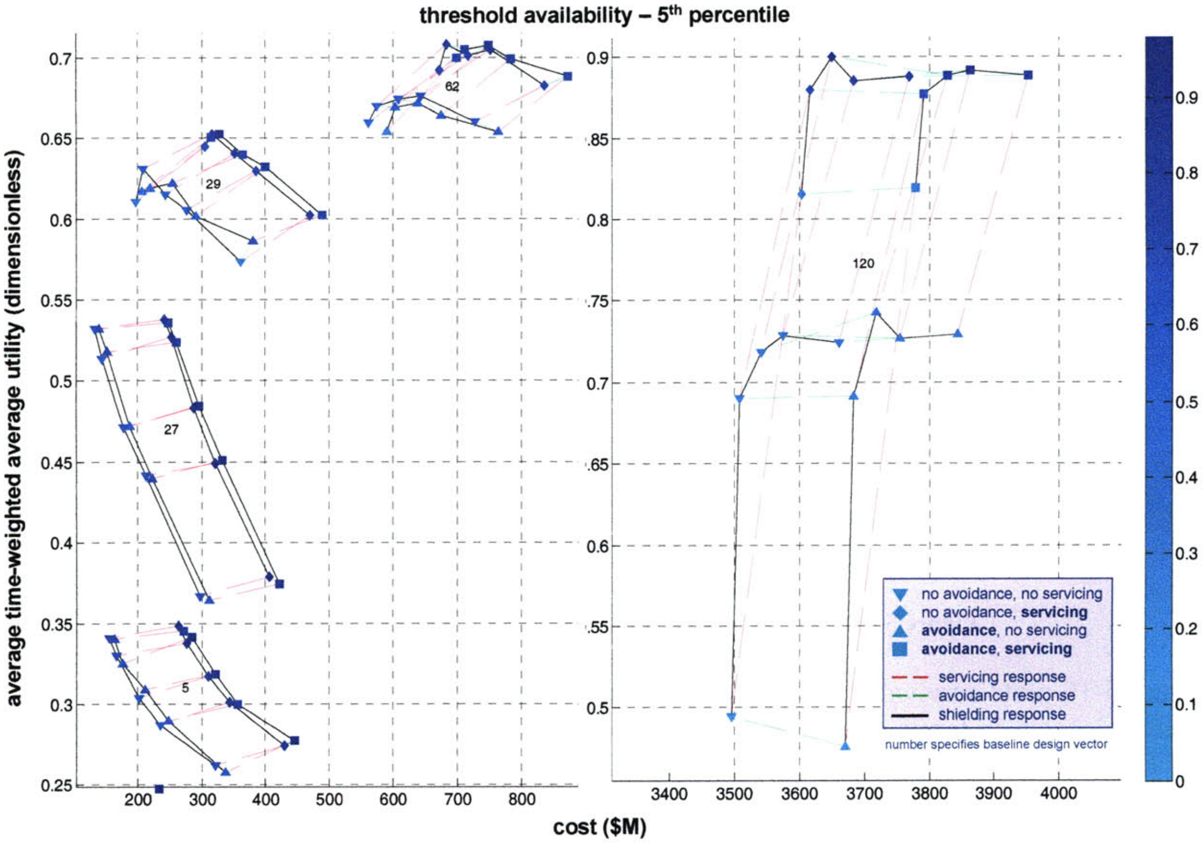


Figure 5-20. Variation in Survivability Response Surfaces

To compare survivability response surfaces in different regions of the tradespace, Figure 5-20 magnifies five low-cost designs and one high-cost design from Figure 5-19. While the width and height of each magnification is conserved to enable comparison, the cost and average utility axes are necessarily different. At this higher resolution, the impact of shielding, avoidance, and servicing on both individual tug designs and different regions of the tradespace can be better observed. Table 5-8 shows the baseline design variable settings for each of the design vectors displayed in Figure 5-20.

Table 5-8. Characteristics of Baseline Design Vectors in Figure 5-20

Baseline Design Vector ID	5	27	29	62	120
Manipulator Capability	Low	Low	Low	Medium	Extreme
Propulsion System	Bi-prop	Electric	Electric	Electric	Nuclear
Propellant Mass (kg)	1200	300	1200	3000	30000

The impact of shielding on average utility and threshold availability is very different across these regions of the tradespace. For baseline design number 5, BD(5), shielding has a negative impact on both cost and average utility while providing no appreciable gains in threshold availability. This is also true of BD(27). The shielding impact on BD(5) and BD(27) stands in stark contrast to BD(120) where the first two increases in shielding mass result in large increases in average utility and threshold availability at only marginal increases in cost. However, after the first two increases in shielding mass in BD(120), survivability benefits diminish while dry mass penalties accumulate. BD(29) and BD(62) represent intermediate cases where the first increase in shielding mass (from 30 to 100 kg) yields slight improvements in average utility and threshold availability before negative returns occur at 300 kg of shielding.

Avoidance does not have much of an impact on survivability in either region of the tradespace. The only general trend observed is the assumed 5% cost penalty associated with incorporating active collision avoidance. Indeed, some designs even occasionally show *losses* in average utility for incorporating active collision avoidance (despite the fact that, as modeled, avoidance can only improve utility trajectories). The limited impact of avoidance is due to the fact that detectable debris encounters (assumed to be >10 cm in diameter) are extremely rare events. Therefore, the avoidance response surface is horizontal to account for the cost penalty while slight, vertical fluctuations may be attributed to random variation over the 500 Monte Carlo trials.

Unlike shielding and avoidance, servicing has a positive impact on average utility and threshold availability across the tradespace. The impact is not uniform, however, as BD(120) (with its higher exposed cross-sectional area) is more susceptible to debris impacts. This space tug is much more likely to experience multiple, non-catastrophic debris impacts over its operational life and therefore benefit substantially from servicing (increasing average utility approximately 25%). Servicing has a smaller positive impact on the lower-end designs, particularly in terms of threshold availability.

5.3.4. Key Insights

The process of developing survivability metrics and applying them within the dynamic survivability model yielded several insights for the space tug tradespace. In terms of space tug survivability, one interesting result is the criticality of the inherent survivability derived from the baseline design vector (before incorporating survivability design variables). For example, selecting baseline tugs with smaller cross-sectional areas has a much greater impact on susceptibility reduction than active collision avoidance. Similarly, increasing grappling capability margin has a greater impact on reducing vulnerability than bumper shielding. Another modeling insight is the extreme sensitivity of the results to the damage model for small- and medium-sized impacts (for which limited empirical data exist). Of all the results, Figure 5-18 is the most interesting from a decision-making perspective as it reveals that the cost-utility Pareto-optimal designs exhibit poor survivability while many highly survivable designs are only slightly dominated in terms of cost and utility.

The customized MATE methodology pursued in the third test case performs well against the five desirable criteria for survivability tradespace studies. First, through the use of "tear" tradespaces and survivability responsive surface plots, the methodology allows integrated trades to be made among cost, performance, and survivability. Second, interactions with the disturbance environment are incorporated across the entire system lifecycle through a stochastic assessment of utility trajectories. Third, path-dependencies in system state are tracked in the dynamic model. Performance against the fourth and fifth criteria remains unchanged from the previous test case: the methodology is amenable to systems at the architecture level (but only tested at the satellite level) and the multi-attribute utility enables a value-centric assessment.

In summary, the third test case indicates that the metrics of time-weighted average utility/utility loss and threshold availability can be applied prescriptively to the evaluation of the survivability of alternative satellite designs. The metrics are unique but interdependent. As illustrated in Figure 5-21, high time-weighted average utility implies high threshold availability (although high threshold availability does not imply high average utility). Taken together, the metrics serve as powerful discriminators of survivability performance.

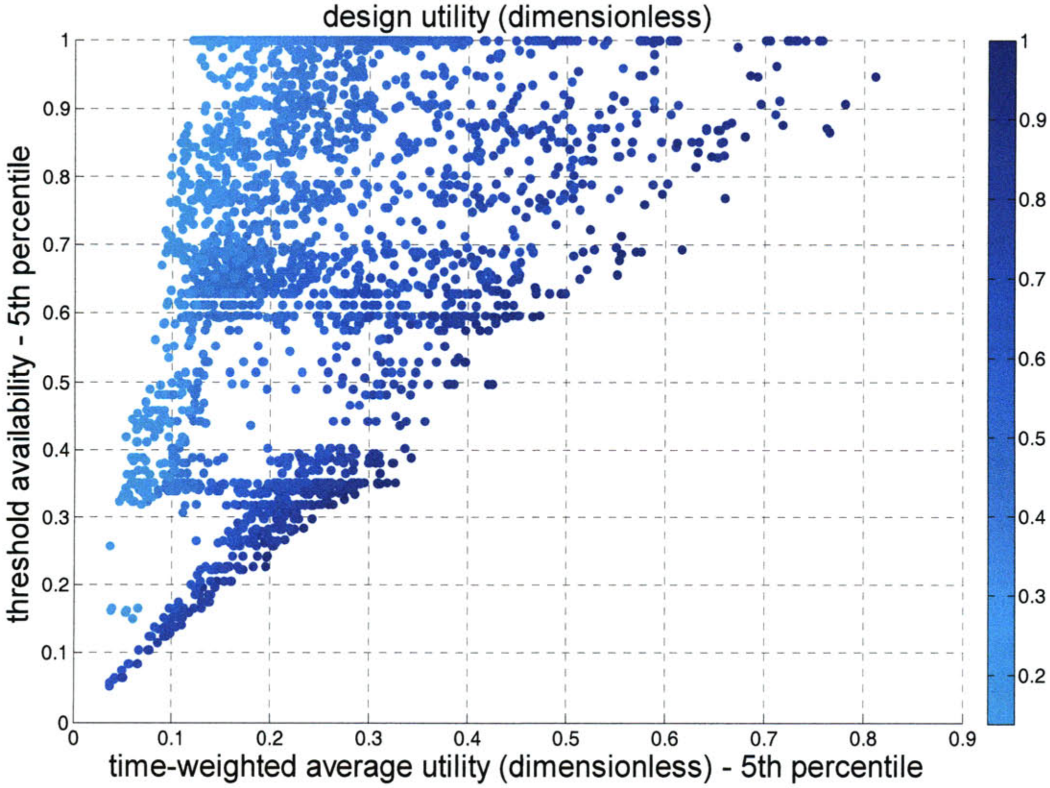


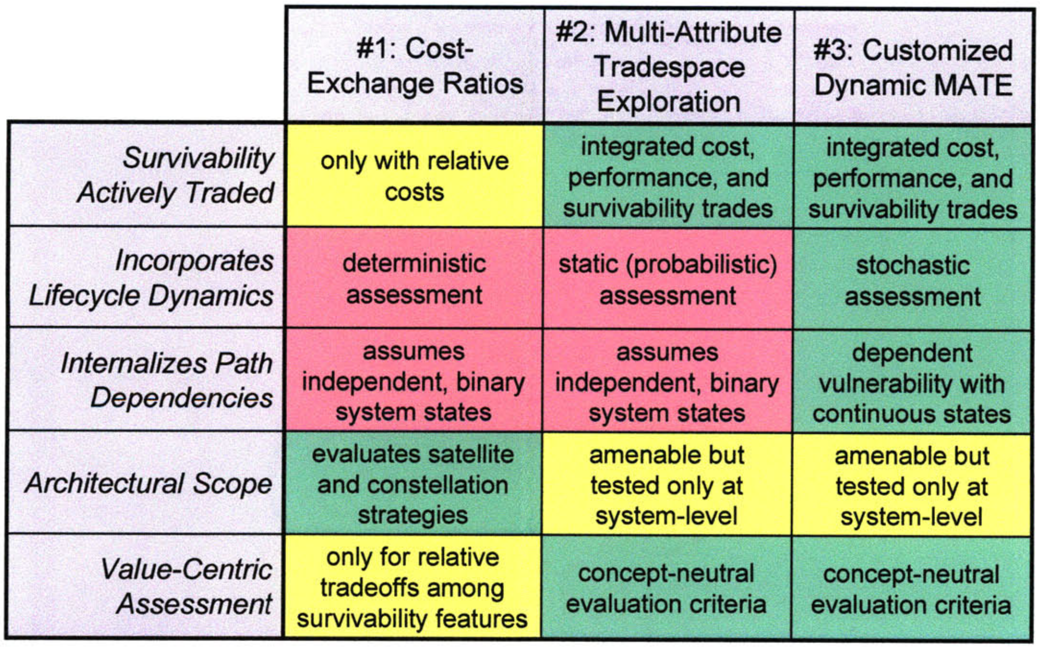
Figure 5-21. Relationship between Time-Weighted Average Utility and Threshold Availability

5.4. Lessons Learned

This chapter described the process of applying existing and proposed survivability metrics to both existing and emerging tradespace analysis methodologies. This process was valuable for obtaining a deeper understanding of the state-of-the practice in survivability analysis (discussed in Chapter 2) and of the challenges associated with operationalizing the conceptualization of survivability (proposed in Chapter 3) in tradespace studies.

Table 5-9 summarizes the evaluation of each test case in terms of the five desirable criteria introduced at the beginning of the chapter. The first test case utilizing cost-exchange ratios performs well in terms of providing an architectural assessment of space-based missile defense but only provided relative insights for comparing across designs. However, neither the lifecycle dynamics of disturbances encounters nor the path dependencies associated with system state are considered. The second test case attempts to incorporate survivability considerations into the emerging MATE methodology. While the strengths of MATE are evident in this test case (*i.e.*, value-based design approach with clear cost-benefit trades), the static nature of the model allows only existing, static survivability metrics to be applied to the tradespace. The third test case builds on the strengths of the second test case while addressing its shortcomings. By following a dynamic MATE approach and implementing a customized system state model, survivability is assessed as a dynamic, continuous, and path-dependent system property

Table 5-9. Evaluation of Survivability Test Cases



	#1: Cost-Exchange Ratios	#2: Multi-Attribute Tradespace Exploration	#3: Customized Dynamic MATE
Survivability Actively Traded	only with relative costs	integrated cost, performance, and survivability trades	integrated cost, performance, and survivability trades
Incorporates Lifecycle Dynamics	deterministic assessment	static (probabilistic) assessment	stochastic assessment
Internalizes Path Dependencies	assumes independent, binary system states	assumes independent, binary system states	dependent vulnerability with continuous states
Architectural Scope	evaluates satellite and constellation strategies	amenable but tested only at system-level	amenable but tested only at system-level
Value-Centric Assessment	only for relative tradeoffs among survivability features	concept-neutral evaluation criteria	concept-neutral evaluation criteria

The third test case demonstrates progress towards a new approach to conducting survivability assessments during early design phases. The survivability metrics of time-weighted average utility loss and threshold availability are shown to be internally valid and the customized implementation of dynamic MATE for the space tug system performed satisfactorily against the five desirable criteria. However, work remains to (1) refine and generalize the dynamic tradespace approach pursued in the third test case into an integrated methodology and (2) demonstrate the prescriptive value of the metrics in trade studies of architectural scope. The following two chapters address each of these respective challenges.

6. Methodology Overview: MATE for Survivability

This chapter addresses the fourth and final research question introduced in Section 1.3.2.

4. For a given space mission, how can alternative system architectures in dynamic disturbance environments be evaluated in terms of survivability?

While the previous chapter focused on the development and verification of metrics for evaluating survivability in tradespace studies, this chapter introduces an end-to-end methodology for system analysts to apply those metrics during conceptual design. In particular, an integrated set of processes is described for incorporating *time-weighted average utility loss* and *threshold availability* within trade studies. The methodology is termed Multi-Attribute Tradespace Exploration for Survivability as it builds upon the legacy MATE process (Section 2.2.2).

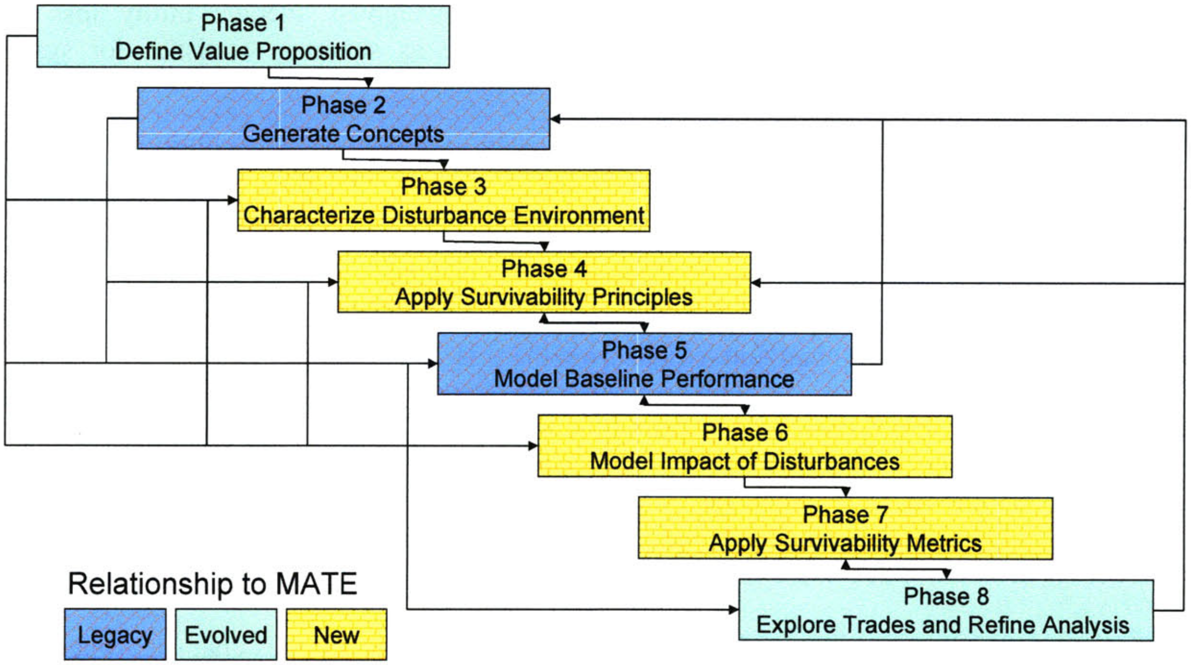

Phase 1
Define Value Proposition
Phase 2
Generate Concepts
Phase 3
Characterize Disturbance Environment
Phase 4
Apply Survivability Principles
Phase 5
Model Baseline Performance
Phase 6
Model Impact of Disturbances
Phase 7
Apply Survivability Metrics
Phase 8
Explore Trades and Refine Analysis
Relationship to MATE
Legacy
Evolved
New

Figure 6-1. Phases of Multi-Attribute Tradespace Exploration for Survivability

The proposed methodology provides system analysts a structured approach for determining how a system can maintain value delivery across operational environments characterized by disturbances. Figure 6-1 provides an overview of the eight phases comprising MATE for Survivability. Arrows illustrate dependencies among the processes, with above diagonal arrows indicating coupled processes with feedback from subsequent phases. Each box is shaded to indicate the relationship of the phase to the legacy MATE process. The phases are briefly described below.

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.

The eight phases of MATE for Survivability follow in sequence but feedback can occur for Phases 2, 4, 5, and 7. In general, feedback is concentrated on the refinement of system concepts (in Phases 2 and 4) based on emergent lessons from the tradespace analysis.

In the eight sections that follow, each phase of the methodology is discussed. After providing a general description and motivation for each phase, specific tasks for each phase are enumerated. To illustrate the methodology, selected examples from the space tug computer experiment are provided throughout the chapter. Following the step-by-step description of the tasks, the overall methodology is summarized in the ninth and final section.

To supplement the introduction to MATE for Survivability provided in this chapter, Appendix E provides a more detailed description of each of the 29 tasks comprising the methodology. In particular, the inputs, outputs, and key activities are described for each task.

6.1. Phase 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 utility function, (1.4) specify emergency value threshold(s), and (1.5) specify permitted recovery time(s).

6.1.1. 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.

6.1.2. Identify Decision-maker

As discussed in Ross et al. (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. 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.

6.1.3. Elicit Multi-Attribute Utility 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.[35] 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 benefit is delivered for exceeding that level). In order to satisfy the axioms of Multi-Attribute Utility Theory (Keeney and Raiffa 1993), the analyst must ensure that the attribute set is defined by the decision-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 benefit 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 (von Neumann and Morgenstern 1953). For systems that have multiple attributes (*N*) with varying weights (*k_i*), computing a single scalar value function that fully reflects decision-maker preferences can be difficult. As a proxy for benefit, the multi-attribute utility function, *$U(\underline{X})$*, as defined in Keeney and Raiffa (1993), is used to reflect preference orderings.

$$\begin{aligned} &KU(\underline{X})+1=\prod_{i=1}^{N}[Kk_iU_i(X_i)+1] \quad \mathit{for} \quad K\neq 0 \\ &\mathit{or} \quad U(\underline{X})=\sum_{i=1}^{N}U(X_i)k_i \quad \mathit{for} \quad K=1 \end{aligned} \tag{6-1}$$

$$\text{where K is the solution to } K+1=\prod_{i=1}^{N}[Kk_i+1]; \text{ and } -1<K<1, K\neq 0. \tag{6-2}$$

[35] Attributes must be complete, operational, decomposable, non-redundant, minimal, and perceived independent (Keeney and Raiffa 1993).

The issue of stakeholder value elicitation is core to the MATE process and well-documented in existing literature. Ross (2003) 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 (2003) discusses the implications of simplifying the elicitation of single-attribute utility functions using hand-drawn utility curves and linear, risk-averse preference relationships.

6.1.4. 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 (Bayer 2007).

As discussed in Section 3.3.4, 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 epochs. A general response to this implication is to elicit applicable multi-attribute utility functions across all potential epochs 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 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 and recovery epochs 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.

6.1.5. 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.

6.2. Phase 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.

6.2.1. Identify Constraints

Constraints are requirements that must be satisfied in order for the system 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 (2006), some constraints are subject to change and must be carefully tracked as shifts may significantly alter the "best" outcome for a particular problem.

6.2.2. 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.

6.2.3. 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 6-1, 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 6-1. Design Value Mapping Matrix – Space Tug

Design Vars	Propulsion System	Fuel Load	Equipment Mass	Total
Attributes				
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 columns and the proposed design variables as rows (or vice versa). 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 rows are summed to provide an estimate of the importance of a particular design variable. (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.)

Fourth, the columns 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.

6.2.4. 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 6-2). 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 6-2. 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

6.3. Phase 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.

6.3.1. 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).

6.3.2. Gather Data on Disturbance Magnitude and Occurrence

Task 3.2 is to gather data on the magnitude and occurrence of different disturbance types to support subsequent model development (*e.g.*, Figure 6-2). 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.

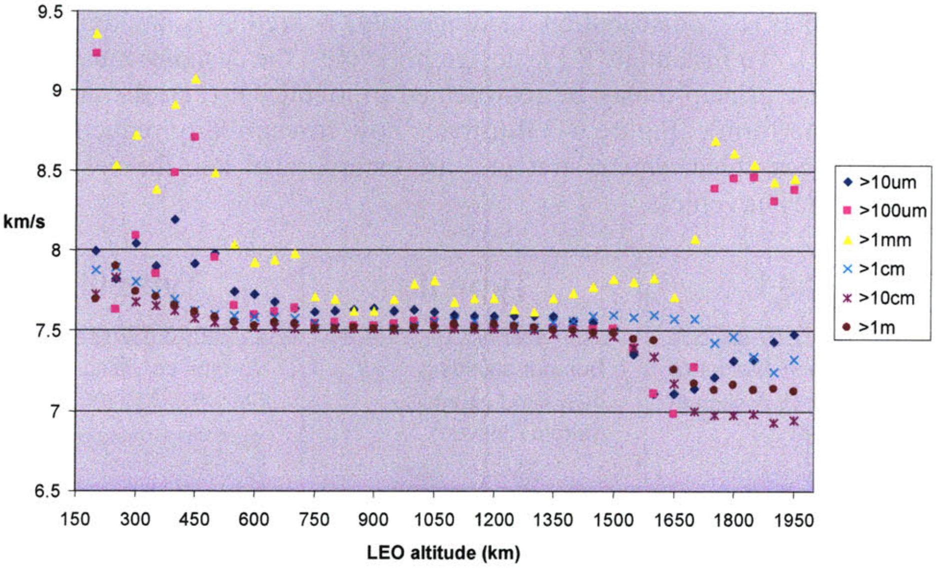


Figure 6-2. Average Orbital Velocity for LEO Debris

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.)

6.3.3. Develop System-Independent Model(s) of Disturbance Environment

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 for applications to all design vector variations within a given system concept.

6.4. Phase 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.

6.4.1. Enumerate Survivable Concepts from Design Principles

The seventeen design principles (Section 4.4) 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 6-3 illustrates how susceptibility reduction, vulnerability reduction, and resilience enhancement strategies are incorporated into the design vector of the "space tug" orbital transfer vehicle.

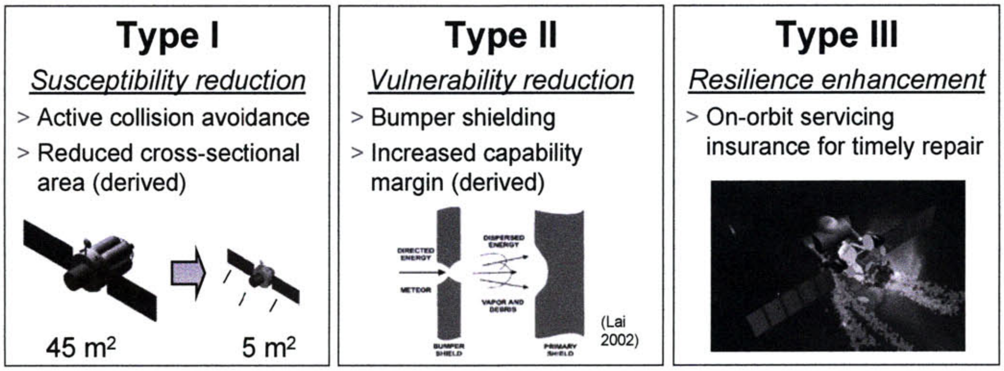


Figure 6-3. Survivability Concepts for Space Tug

6.4.2. Parameterize Survivable Concepts with Design Variables

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.

6.4.3. Assess Ability of Design Variables to Mitigate Disturbances

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 used.

6.4.4. 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.

6.4.5. Finalize Design Vector

Finalizing the design variables is required before modeling and simulating the design alternatives. 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 associated with 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). For example, Table 5-5 shows the final design vector for space tug.

6.5. Phase 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 vectors 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.

6.5.1. 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 6-3). Modules within the matrix enable the model to be decomposed to enable parallel development.

Table 6-3. N-squared 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	■

6.5.2. 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.

6.5.3. 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 (Wertz and Larson 1999).

6.5.4. 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.

6.6. Phase 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 dynamically characterizing system performance from a path-dependent, 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.

6.6.1. Calculate Stochastic Susceptibility

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), a system-dependent model of the disturbance environment is created (*e.g.*, debris flux as a function of mass per exposed cross-sectional area). For example, Figure 5-9. Conjunction Outcomes, shows the baseline susceptibility of the 2560 designs in the space tug tradespace. If disturbances occur probabilistically, a Monte Carlo analysis is conducted to generate representative distributions of disturbance timelines for the design vectors.

6.6.2. 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 5-6. Debris Impact Outcomes). The vulnerability model takes the form of a probabilistic lottery in which multiple runs are required to extract the distribution of potential outcomes. Although static, the vulnerability model is only activated 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.

6.6.3. 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 takes the form of 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.

6.6.4. Generate Distributions of Utility Trajectories

As defined in Chapter 3, 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 incorporates 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.

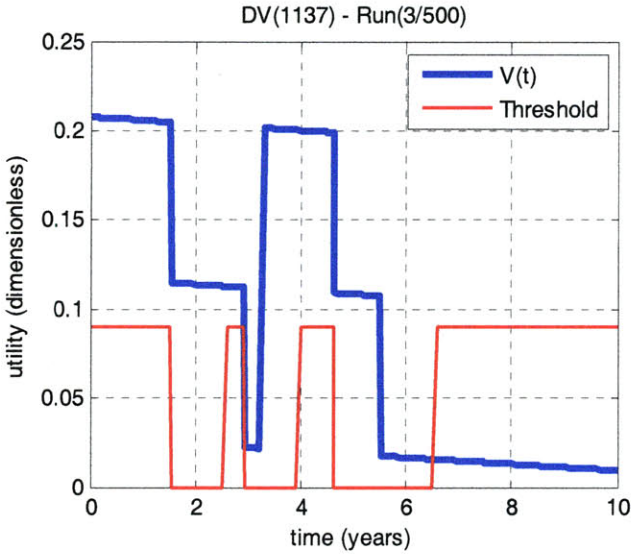


Figure 6-4. Sample Utility Trajectory Output from Dynamic State Model

The dynamic space tug model demonstrates the definition of survivability by simulating utility trajectories of alternative designs in the presence of orbital debris events. Figure 6-4 presents a sample utility trajectory output from the model, illustrating *V(t)* (*i.e.*, dynamic multi-attribute utility) over a possible ten-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 distribution of potential system lifecycles. Therefore, a Monte Carlo analysis is conducted by running the simulation until a representative distribution of utility trajectories is generated.

Determining the appropriate number of Monte Carlo trials requires a trade-off between the accuracy of the reported survivability metrics and computing time. While 1,000 is a typical baseline for the number of trials to consider, the complexity of the calculations may require more or less trials to be performed (Hazelrigg 1996). To determine the number of trials, it is advisable to conduct a convergence study on a small number of design vectors to examine the sensitivity of the reported survivability metrics to the number of Monte Carlo trials. For example, Figure 6-5 shows how 5th percentile threshold availability for one design vector varied as a function of the number of Monte Carlo runs in one set of simulations. While smaller runs (*e.g.*, 100 trials) diverge considerably from the most accurate estimate of 20,000 trials, 500 trials achieve a good balance between accuracy and computing time. Therefore, 500 runs were conducted for each design vector before reporting the median time-weighted utility loss and 5th percentile threshold availability in the tear tradespace (Figure 5-17). Precisely understanding the variance of the reported survivability metrics is particularly critical if the tear tradespace is subsequently filtered for Pareto efficiency.

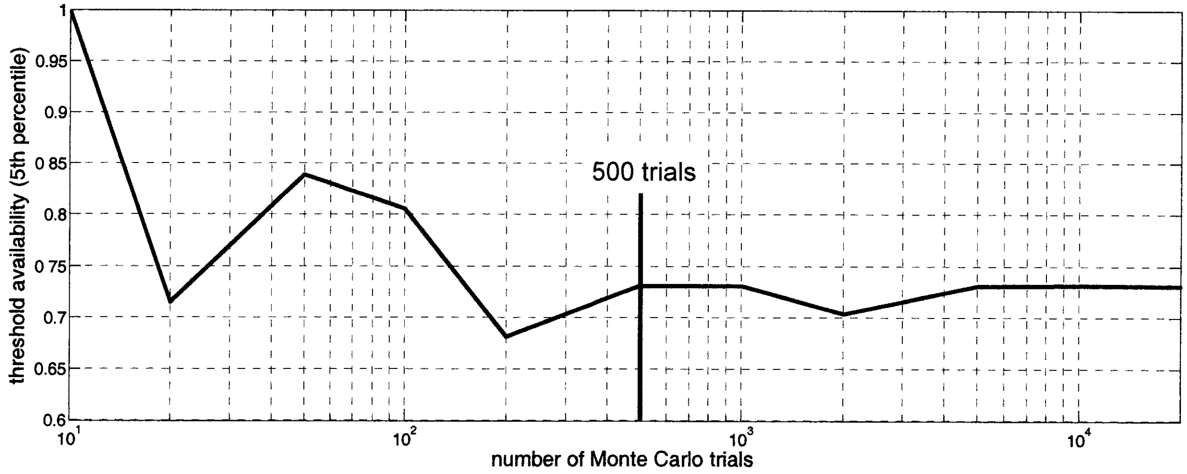


Figure 6-5. Monte Carlo Convergence for One Design Vector

Having modeled the impact of disturbances on system lifecycles and generated distributions of utility trajectories for each design vector, the next challenge is to distinguish across distributions 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.

6.7. Phase 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 introduced in Section 3.3 are briefly reviewed.

The survivability metrics evaluate 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:

$$\overline{U}_L = U_o - \frac{1}{T_{dl}} \cdot \int U(t)\ dt \tag{6-3}$$

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 of the ability of systems 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 time above thresholds *TAT* to the total design life:

$$A_T = \frac{TAT}{T_{dl}} \tag{6-4}$$

6.7.1. 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 and threshold availability, introduced in Chapter 3, 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 an 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 itself through the selection of lower percentiles). Selection of the percentile reporting levels is an iterative process with Task 8.1, Conduct Integrated Tradespace Exploration.

6.7.2. Calculate Time-Weighted Average Utility and Threshold Availability

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. For example, see Figure 5-14. Distributions of Time-Weighted Average Utility and Figure 5-15. Sample Distribution of Threshold Availability.

6.8. Phase 8: Explore Tradespace

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

6.8.1. Conduct Integrated Cost, Utility, and Survivability Trades

The purpose of tradespace exploration is to map the decision-maker preferences in the value domain onto the space of possible designs in the technical 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 identified for more detailed analysis.

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 tradespace representation. Decision-makers may navigate the tradespace by examining designs near the top-left (high utility, low cost) with high availability (darker) and minimal utility loss (shorter tail). For example, Figure 6-6 presents a survivability tear tradespace from space tug in which designs at the Pareto-surface of cost, utility, and utility loss are displayed.

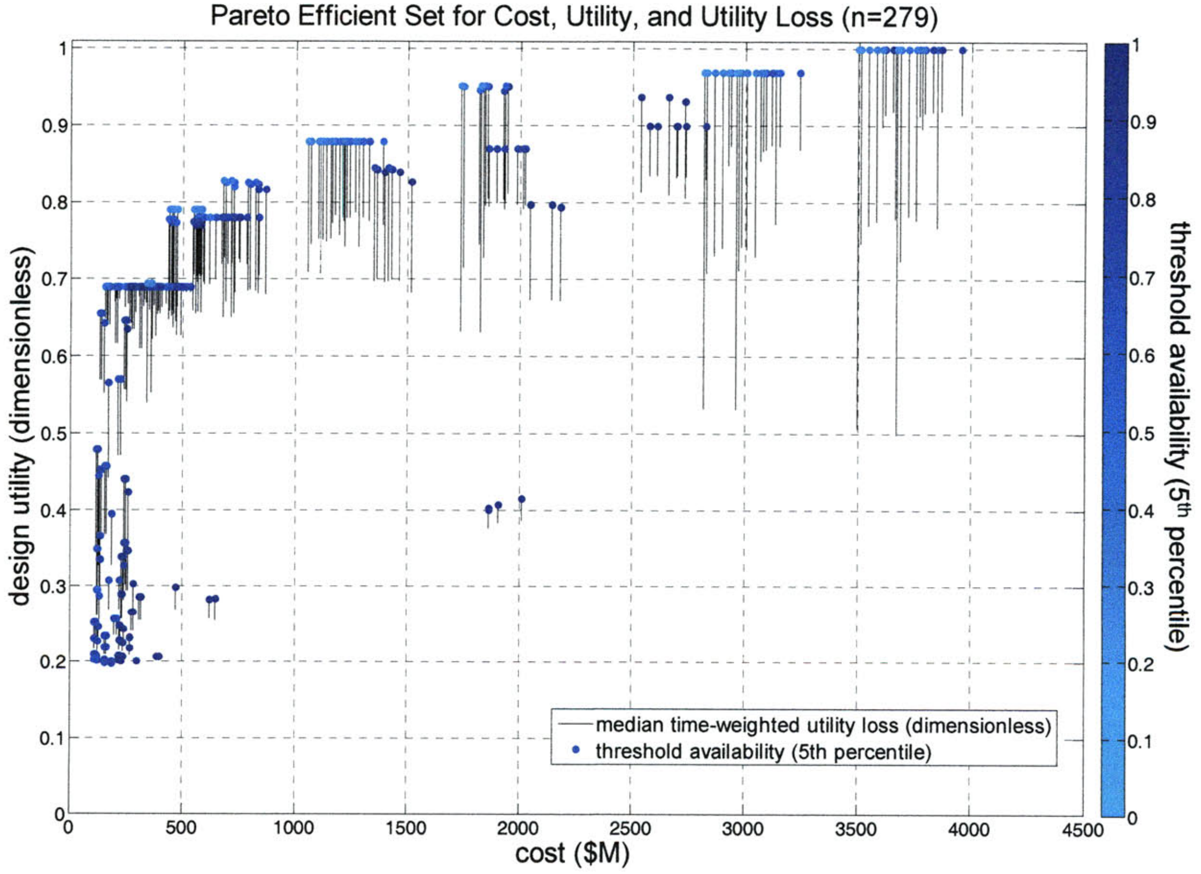


Figure 6-6. Three-Dimensional Pareto Surface of Survivability Tear Tradespace

6.8.2. 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 smaller number of design vectors for higher-fidelity modeling. For example, Figure 6-7 shows how a survivability response surface analysis may be conducted to assess how the 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.

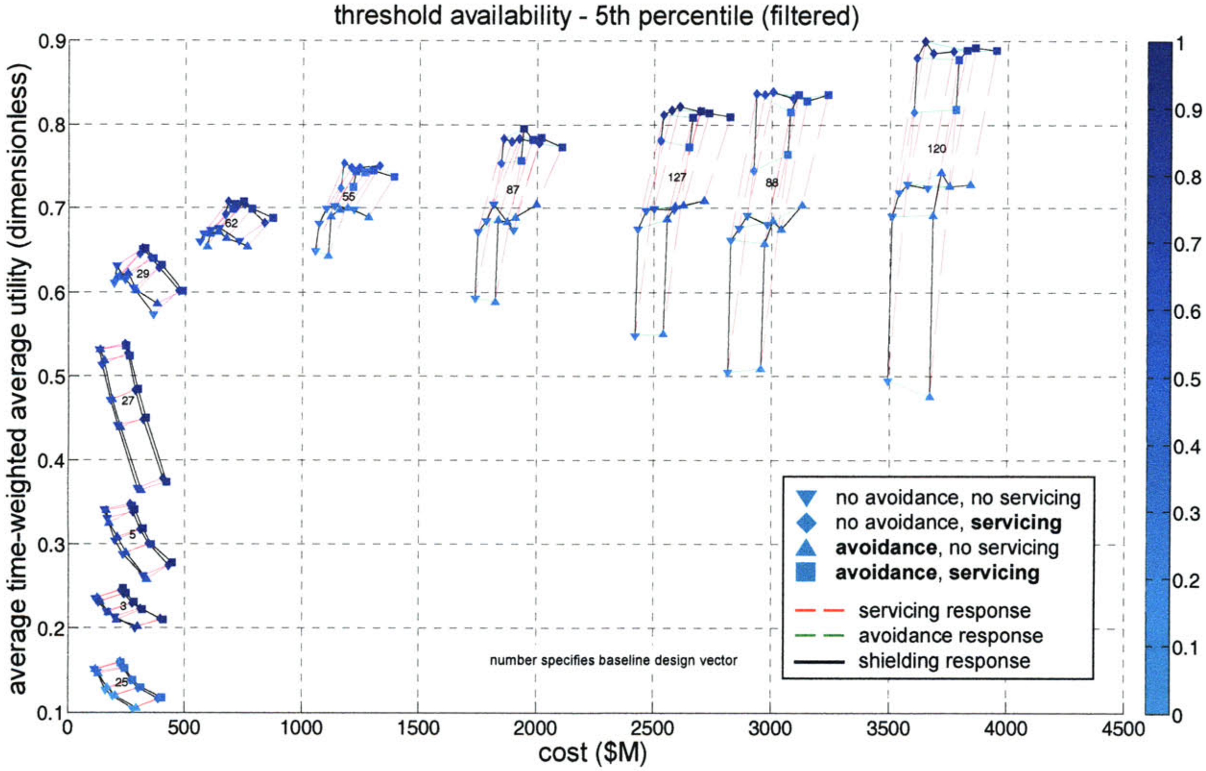


Figure 6-7. Survivability Response Surfaces along Pareto-Front of Cost and Average Utility

6.9. *Synthesis*

The 8-phase, 29-step process introduced in this chapter provides a structured approach to the evaluation of the survivability of design alternatives that will be operating in dynamic disturbance environments. 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 metrics. In particular, the MATE for Survivability approach 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 6-8 provides a flow chart of the process and identifies relationships with the legacy MATE process.

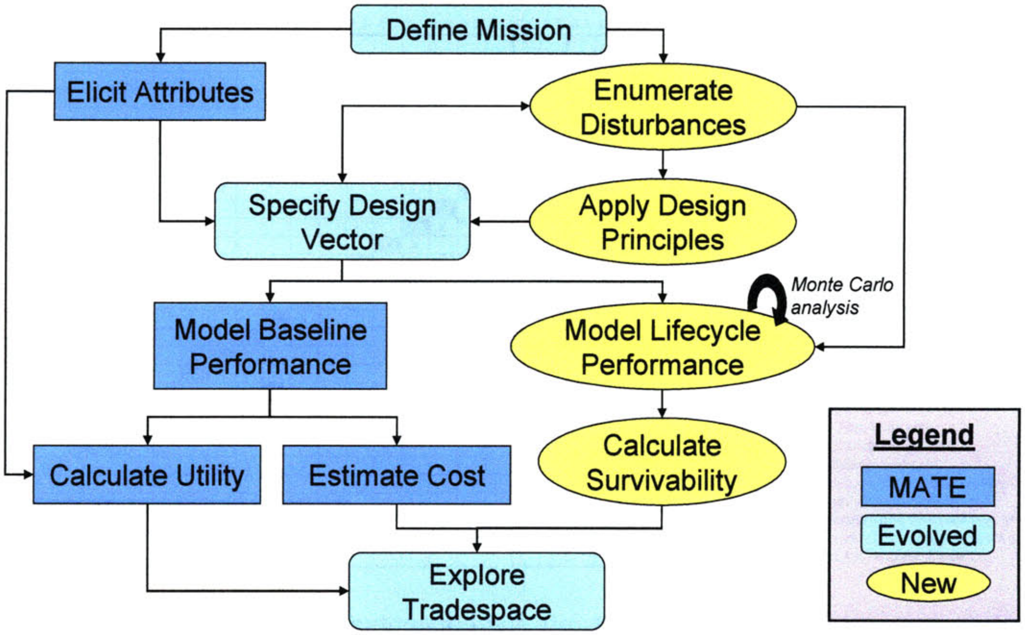


Figure 6-8. Multi-Attribute Tradespace Exploration (MATE) for Survivability

Both the survivability design principles and metrics 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 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. In applying the design principles to space tug, many latent survivability trades were found within the baseline set of design variables. The process provides an explicit means for recognizing these latent trades and informing utility-survivability interactions. Application of the survivability metrics to subsequent tradespace exploration allows these interactions to be quantified and traded by the decision-maker.

Table 6-4 provides a Task Structure Matrix of each of the 29 steps within MATE for Survivability as well as a bird's-eye view of the dependencies among tasks. Each row consists of a particular task with "X" marks specifying inputs to that task. The "X" marks in the upper-right region (above the diagonal of solid black boxes) indicate feedback from subsequent tasks (*e.g.*, 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 6-4 underscores the importance of pursuing modeling and simulation activities at a level of fidelity that is consistent with the ability to conduct several iterations of the overall process.

Table 6-4. 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 utility 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	■

Incorporating survivability considerations into the conceptual design phase 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 the design process.

7. Case Application: Satellite Radar

This chapter applies Multi-Attribute Tradespace Exploration for Survivability (Chapter 6) to an analysis of potential future military satellite radar constellations. Given the repeated attempts over the past decade by the U.S. military to acquire a satellite radar capability and the tens of billions of taxpayer dollars at stake, satellite radar offers a promising subject both to test the proposed survivability analysis methodology and to gather prescriptive insights to inform ongoing trade studies. Following an introduction to the history of satellite radar and a discussion of the scope of the analysis in Section 7.1, each phase of MATE for Survivability is applied in Section 7.2. The chapter concludes in Section 7.3 with a discussion of the implications of the case application for satellite radar and for the underlying methodology.

7.1. Introduction to Satellite Radar

This section provides a brief introduction to contextualize and motivate the application of MATE for Survivability to satellite radar (SR). After describing the military value of SR, the advantages and disadvantages of transitioning the airborne radar surveillance mission to space are discussed in Section 7.1.1. An overview is also provided of recent attempts by the U.S. military to acquire a satellite radar capability. In section 7.1.2, the scope of the SR case application is outlined. A notional SR enterprise diagram is introduced, informing the enumeration of dynamic context factors that, while exogenous to the control of the SR program manager, are critical to program success. Finally, the relationship between the SR case application and ongoing collaborative work at MIT's Systems Engineering Advancement Research Initiative is described.

7.1.1. Historical Context

Radio detection and ranging (radar) is the process of transmitting modulated waveforms using directive antennas to search for targets within a volume of space. Under ideal conditions, electromagnetic energy travels through space in a straight line at a constant speed. If the energy meets an electrically leading surface, waves are reflected and the reflections are picked up by the receiving antenna. The reflections or "echo" may be processed to extract target information. The presence of a reflected signal is used to detect targets while the angle of reflection indicates the direction of the target. The time delay between the transmitted signal and received signal provides range. The spectrum of the received signal indicates the target velocity using the Doppler shift. Moving targets against a stationary background may also be detected using the spectrum of the received signal.

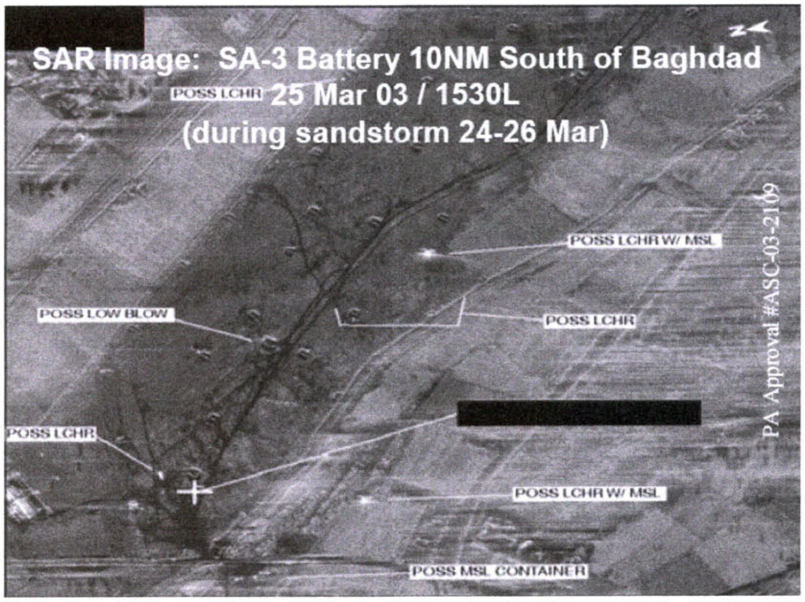


Figure 7-1. Synthetic Aperture Radar Image Acquired During a Sand Storm (Chang and Bender 2005)

As active sensors, radars enable all-weather detection of forces, providing tremendous value to military users operating in harsh environments (Figure 7-1). Developed over the first half of the 20th century, radar's military benefit was first fully realized by the British during the Second World War in homeland defense against German air attacks. The line-of-sight visibility of radar has driven militaries to deploy radars at increasingly higher vantage points (Corcoran 2000). The U.S. military currently deploys radars on a variety of aircraft systems (*e.g.*, E-8C Joint Surveillance Target Attack Radar System [JSTARS], E-3 Sentry Airborne Warning and Control System [AWACS]) and uninhabited aerial vehicles (*e.g.*, MQ-1 Predator, RQ-4 Global Hawk).

In the 1990's, several studies were conducted on moving the airborne surveillance mission to orbital platforms (Wickert, Shaw and Hastings 1998; DeLap 1999; Preiss, Fiedler and Kellett 1999). For example, the 1995 Space Sensors Study investigated the feasibility of transitioning the JSTARS mission of ground-moving target identification (GMTI) and the AWACS mission of air-moving target identification (AMTI) to space (DeLap and Suhr 1996). The study found that the required satellite masses would be prohibitively expensive given 1995 technology and recommended allowing emerging commercial telecommunications systems to mature enabling technologies.

There are several advantages associated with space-based radar surveillance (DeLap and Suhr 1996; Corcoran 2000). First, the higher vantage point enables superior performance in the coverage rate of a given area. Depending on orbital altitude and constellation density, satellite platforms may offer continuous line-of-sight of the entire globe. Second, space systems provide access to denied areas far behind enemy lines. This access offers high elevation angles that may mitigate terrain masking. Third, in contrast to airborne systems, satellites are always on-station to support near real-time tasking. Fourth, the space-basing of radar sensors improves operator survivability. Controllers in U.S.-based ground stations replace vulnerable pilots and eliminate the need for the overseas deployment of large maintenance crews.

There are also several disadvantages associated with space-based radar surveillance. First, significantly more power is required at orbital altitudes given that the received power decreases as the inverse of the altitude to the fourth power. Ignoring losses, the equation for received power, P_e, is given in terms of transmitted power, P_t, antenna gain, G, wavelength, λ, target cross section, σ, and range, R.

$$P_e = \frac{P_t \cdot G^2 \cdot \lambda^2 \cdot \sigma}{(4\pi)^3 \cdot R^4} \tag{7-1}$$

Second, individual satellites are unable to loiter and maneuver above targets (given the drive for lower orbital altitudes to cope with the radar range equation and the extreme ΔV penalties associated with maneuvering in LEO). Therefore, large numbers of satellites may be required to provide continuous coverage over small geographic areas. Third, there is likely to be no opportunity for the satellites to be repaired or upgraded (other than software updates) over their operational lives. As a result, design lives are likely to be much shorter than airborne alternatives. Fourth, as articulated in Section 1.2.3, satellite survivability is an issue given the proliferation of threats to space systems. The fifth and final disadvantage of space-based radar surveillance is the extensive risk associated with technology development (*e.g.*, deployable active electronically scanned arrays [AESA], lightweight solar arrays, space-time adaptive processing) (Davis 2003).

Over the past decade, there have been several attempts by the U.S. military to acquire a capability for space-based radar surveillance. In 1998, the Air Force and several other agencies initiated the Discover II program to demonstrate GMTI in space with direct in-theater tasking and downlink. As a precursor to the launch of a 24-satellite constellation, two prototype satellites equipped with 40 m^2 AESA radars operating at 10 GHz were to be launched into 770 km circular orbits with a 53° inclination. The target unit production cost was $100 million with a target 20-year lifecycle cost of $10 billion (CBO 2007). However, the system was cancelled in 2000 due to its uncertain costs and schedule, poorly explained requirements, and lack of operational concepts and trade-off analysis (Tirpak 2002). Following cancellation, Discoverer II was reborn in 2001 as a new acquisition program called Space-Based Radar. Using the same technology as Discoverer II, Space-Based Radar intended to follow a spiral development model with an initial operational capability by 2010. However, the program was effectively killed in the 2005 Defense Appropriations bill when lawmakers provided just $75 million of the $327 million requested by the President's budget (Singer 2004). In a repeat of history, the program was restructured again in 2005 and renamed Space Radar. Following the "back-to-basics" acquisition model of focusing on technology development before system development, Space Radar intended to have an initial operating capability by 2015. Citing a lack of affordability, the program was cancelled for a third time in March 2008 (Clark 2008). While technology development continues, there is currently no formal acquisition program for military satellite radar.

In summary, radar systems provide unique all-weather reconnaissance and surveillance capabilities. Transitioning radar sensors from airborne to space platforms is challenging given the range requirements and strict size, weight, power, and reliability requirements imposed by satellites. Over the past decade, military satellite radar programs have faltered due to immature technology as well as due to fractured management among system acquirers. Given these historical lessons, future analyses of satellite radar should emphasize front-end systems engineering activities. Such activities should include defining operational utility across stakeholders, exploring the multi-dimensional tradespace offered by alternative radar designs and constellation structures, and assessing the impact of future contextual uncertainties (*e.g.*, environmental disturbances) on performance over the entire system lifecycle.

7.1.2. Scope of Analysis

As reported by the Congressional Budget Office (2007), future satellite radar systems are intended to carry out four missions: (1) synthetic aperture radar (SAR) imaging, (2) ground moving-target identification, (3) three-dimensional terrain mapping, and (4) open-ocean surveillance. This mission set excludes the AMTI mission, which is 100 to 1000 times more difficult than the GMTI mission for similar radars (Table 7-1).

Table 7-1. Order-Magnitude Comparison of GMTI to AMTI (Davis 1999)

	GMTI	AMTI	Difference (dB)
Target RCS	10	0 to -10	10 to 20
Revisit Rate (sec)	30	10	5
Volume coverage	X	3X	5
			Δ20-30 dB!

In applying the MATE for Survivability process to satellite radar in this chapter, the focus is on the GMTI mission. Past analyses of satellite radar alternatives have focused on the SAR imaging and GMTI missions because they are considered the highest priority for the new system and because detecting and tracking targets on the ground should be more difficult than detecting and tracking targets at sea (CBO 2007). In this analysis, the decision was made to assess operational utility in terms of GMTI in order to focus the analysis on survivability considerations for a single military decision-maker rather than introduce multi-stakeholder tensions across users of SAR and GMTI.[36]

[36] See Ross (Ross 2006) for one approach for incorporating multi-stakeholder considerations into MATE and Ross et al. (2008) for a specific application of the methodology to competing stakeholders in satellite radar.

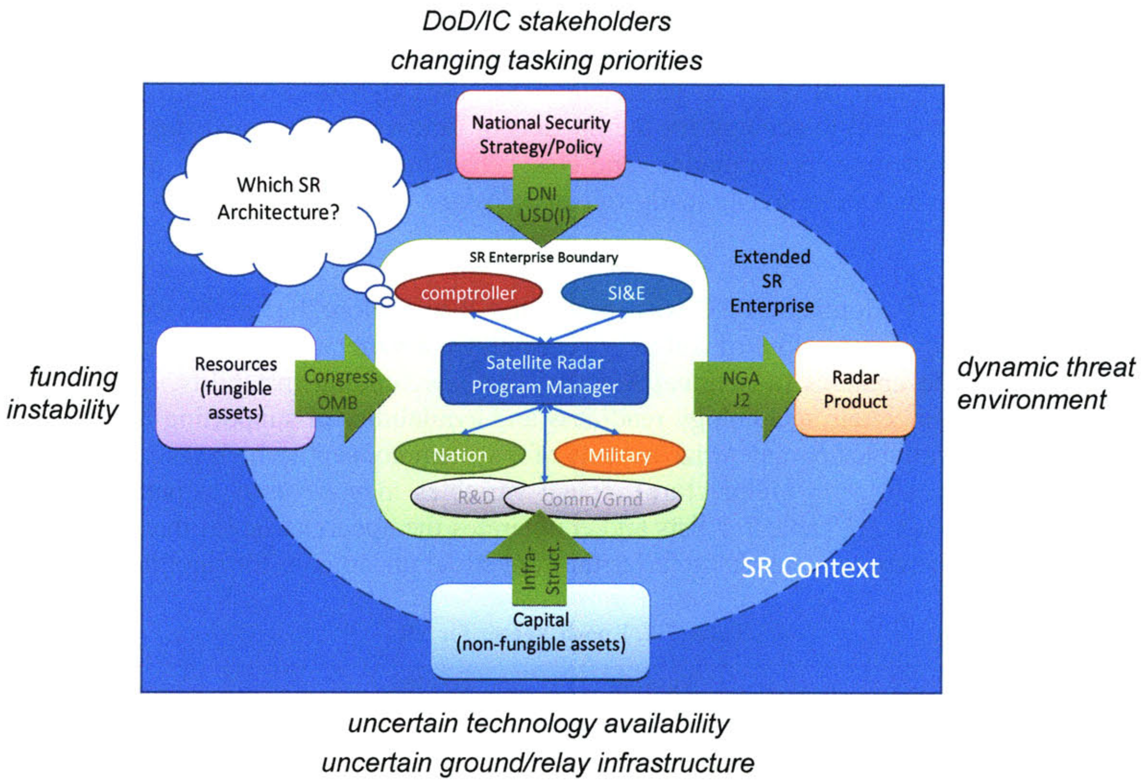

DoD/IC stakeholders
changing tasking priorities
National Security Strategy/Policy
Which SR Architecture?
DNI
USD(I)
SR Enterprise Boundary
comptroller
SI&E
Extended SR Enterprise
funding instability
Resources (fungible assets)
Congress
OMB
Satellite Radar Program Manager
NGA
J2
Radar Product
dynamic threat environment
Nation
Military
R&D
Comm/Grnd
Infra-Struct.
SR Context
Capital (non-fungible assets)
uncertain technology availability
uncertain ground/relay infrastructure

Figure 7-2. Satellite Radar Enterprise

As discussed in Chapter 6, an important task preceding formal attribute elicitation from the decision-maker is to clearly establish the boundaries for system development and operation. Figure 7-2 presents an enterprise diagram of a notional satellite radar (SR) system. Traditionally, such a diagram may be used to narrow the scope of analysis by informing what parameters are under the control of the design team and what factors are exogenous to the system boundary. As illustrated by the four boxes within the SR context, there are several exogenous factors that affect the value delivered by SR, yet are outside of the control of the SR program manager.[37]

To better identify, quantify, assess, and manage the risks of developing complex space systems, the MIT SEAri research group collectively developed the Responsive Systems Comparison method (RSC) in 2008 to evaluate the ability of systems to deliver value across changing future

[37] Figure 7-2 illustrates four types of dynamic uncertainty that are exogenous to the control of the SR program manager: mission needs (*i.e.*, Strategy/Policy), funding (*i.e.*, Resources), supporting infrastructure (*i.e.*, Capital), and operational environment (*i.e.*, Radar Product). First, any SR system will be designed, developed, and operated within a complex institutional environment with multiple stakeholders and competing priorities. For example, the importance of SAR imaging relative to GMTI may drive the system development in different directions. Second, given the long development times of space systems, the annual funding allocations for SR are uncertain over the development lifecycle. Third, the supporting infrastructure for the SR platforms will directly impact the system value delivery. Supporting infrastructure may include the availability of technologies (typically developed and matured in research and development organizations) as well as system-of-systems considerations. For example, the future availability of the transformational satellite communications system or collaborative airborne intelligence, surveillance, and reconnaissance platforms will directly affect the operational value of the SR system. Fourth, the operational environment of the SR system is also highly uncertain (*e.g.*, adversary tactics) and directly impacts the value delivery of the SR system.

contexts (Ross, McManus et al. 2008). RSC builds on the MATE approaches of aligning stakeholder value elicitation with the designs under consideration and of the broad evaluation of thousands of design alternatives. In particular, RSC uses dynamic, value-driven tradespace exploration (Section 2.2.2) to account for the impacts of time-varying contexts and requirements on program cost, schedule, performance, and risk. The intent of RSC is to allow decision-makers to recognize and value dynamically-relevant designs while operating with limited design resources.

Concurrent with its development, RSC was applied to SR to explore the sensitivity of alternative architectures to the distribution of future uncertainties enumerated in Figure 7-2. These uncertainties include changes to national security strategy, funding instability, dynamic threat environments, and uncertain technology readiness and availability of supporting infrastructures. Just as the design variables parameterize aspects of a system concept (which taken together as a set uniquely define a system architecture), epoch variables may be used to parameterize and define a system context.[38] Table 7-2 lists and enumerates the epoch variables that were selected by the RSC development team to characterize the contextual uncertainty for satellite radar.[39]

Table 7-2. Epoch Vector for SR

Epoch Variable Category	Epoch Variables	Number of Steps	Enumerated Range	Units/Notes
Strategy/Policy	Imaging vs. Tracking Utility Expectations	3	[1,2,3]	1=SAR<GMTI 2=SAR=GMTI 3=SAR>GMTI
Resources	Budget Constraint	na	na	Use tradespace to vary "costs"
Capital	Radar Technology	3	[1,2,3]	1=Mature 2=Medium 3=Advanced
Capital	Communication Infrastructure	2	[1,2]	1=AFSCN 2=WGS+AFSCN
Captial	Collaborative AISR Assets	2	[1,2]	1=Available 2=Not available
Radar Product	Operations Plans	9	[9,19,44,45,49,60,84,94,103]	Lookup table of geographic region & target op. plans
Radar Product	Threat Environment	2	[1,2]	1=No jamming 2=Hostile jamming

[38] Given the exogenous uncertainties characterizing the context and stakeholder expectations over the SR system lifecycle, RSC seeks to identify value-robust designs by incorporating broad distributions of plausible future context states. In particular, rather than making static assumptions regarding each uncertainty or assuming fixed worst-case values, the future context states are parameterized using an epoch vector. In a process analogous to the parametric concept generation phase in a traditional MATE analysis, each key uncertain system exogenous factor is characterized by an epoch variable. An epoch variable is a quantitative parameter that reflects an aspect of an uncertain future context. Each possible combination of epoch variables constitutes a unique epoch vector, and the set of all possible epoch vectors constitutes the set of state-scenarios. While epoch variables are not directly under the control of the program manager, the probability of some epoch variable levels from arising may be influenced by the program manager (*e.g.*, research and development dollars on technology readiness).

[39] When proposing epoch variables and enumeration ranges, a natural tension exists between including more variables to analyze larger sets of plausible futures and the computational limits on evaluating a larger set of scenarios. Iterative structured and unstructured interviews were conducted with domain experts representing stakeholders from the four areas of system exogenous uncertainty identified in the satellite radar enterprise diagram (Figure 7-2). Based on those discussions the epoch variables for the SR system context were derived and are shown in Table 7-2.

While the Responsive Systems Comparison method was developed to address the general challenge of incorporating dynamic system contexts into tradespace exploration, the focus in this chapter is on incorporating survivability considerations given uncertain operational environments. Table 7-2 shows that a limited number of environmental factors were incorporated into the RSC analysis (*e.g.*, jamming, availability of relay backbone). However, other environmental factors were not considered (*e.g.*, debris), and dedicated survivability design variables were not incorporated into the tradespace (*e.g.*, shielding). By incorporating these survivability considerations using MATE for Survivability, the SR case application in this chapter serves as both a specialization and an extension of the analysis of satellite radar alternatives performed by SEAri using RSC.[40]

7.2. Application of MATE for Survivability

7.2.1. Phase 1: Elicit Value Proposition

The attributes and utility functions for GMTI are based on the decision-maker value elicitation by the RSC development team. In this process, attributes (*i.e.*, quantifiable parameters for measuring how well decision-maker-defined objectives are met) are extracted from the mission statement in addition to associated acceptability ranges, single-attribute utility curves, and a multi-attribute aggregation.

The attributes are intended to operationalize the general objectives of the mission statement:

The purpose of the analysis is to assess potential satellite radar architectures for providing the United States Military a global, all-weather, on-demand capability to track moving ground targets. The system should provide situational awareness to support tactical military operations while maximizing cost-effectiveness and surviving disturbances in the natural space environment.

In probing decision-maker needs for objective statements, the concept-of-operations for the system is discussed to structure and clarify the process of defining attributes. This scenario-based dialogue helps to place the decision-maker in the proper mindset for the attribute elicitation. Figure 7-3 provides an illustration of the satellite-level concept-of-operations for satellite radar. In particular, satellites in a Walker constellation perform the GMTI mission by observing donut-shaped areas on the surface of the Earth. The field-of-regard for each satellite is limited by specifying minimum and maximum grazing angles within which the Doppler shift of moving targets may be detected. While satellites may be limited in their ability to look forward or backward (removing two wedges from the circle), it is assumed in the model that the satellite will be able to rotate 360° for full visibility. By optimizing the radar search to the target deck input to the model, the attributes of a given design alternative may be calculated.

[40] The RSC development overlaps with MATE for Survivability in three phases: (1) value elicitation, (2) concept generation, and (3) modeling of baseline (static) system performance.

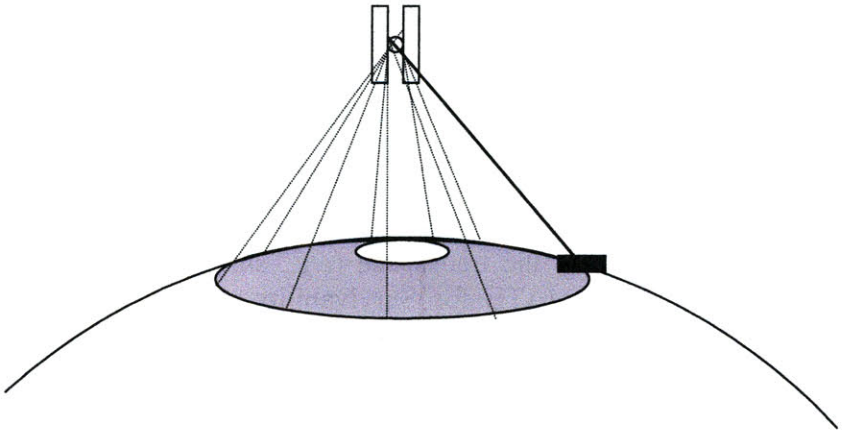


Figure 7-3. SR Concept-of-Operations

Given this concept-of-operations for satellite radar, six attributes for the GMTI mission were derived from interview data: (1) number of target boxes, (2) minimum detectable target velocity, (3) minimum detectable radar cross section, (4) target acquisition time, (5) track life, and (6) tracking latency. These attributes provide quantitative performance metrics that can be used to define mission utility for a tactical military user.[41] While the former three attributes are satellite-level properties that characterize the performance of the radar sensor, the latter three attributes characterize constellation performance (*i.e.*, their calculation is dependent upon cooperation among system nodes in the overall architecture).

Table 7-3 defines the six attributes and provides ranges of acceptability. Each attribute delivers zero utility when it is at the "worst" value that is still acceptable to the stakeholders. A utility of one is reached when the stakeholders are fully satisfied. Increasing utility (from 0 to 1) is indicated in Table 7-3 by the direction of the arrows. As illustrated by the subsequent single-attribute utility functions, attributes that range over many orders of magnitude tend to be logarithmically related to utilities, while attributes that have narrower ranges are generally linearly related to utilities.

[41] The attributes are translated to a utility function using multi-attribute utility methods (Keeney and Raiffa 1993). While formal methods exist for eliciting the mapping of attributes to utilities by interviewing stakeholders (*i.e.*, single-attribute utility functions), these methods are resource-intensive. Since multi-attribute utility methods are not part of the RSC development effort, utility elicitation is simplified in this case application whereby the attribute set is based directly on interview data and the acceptability ranges and single-attribute utility functions are based on order-of-magnitude estimates by the RSC development team.

Table 7-3. SR Attributes (GMTI)[42]

Attribute	Definition	Acceptable Range
number of target boxes	number of 200x200 km target boxes (consisting of targets with a given velocity and radar cross section) that can be imaged by a single satellite during a single pass	0 → 6
minimum detectable velocity (m/s)	lowest possible velocity of a target that can be detected from the backdrop of its surroundings	5 ← 50
minimum detectable radar cross section (m^2)	minimal target area capable of reflecting a signal detectable by the radar's receiver in response to a radar pulse	0.01 ← 1000
target acquisition time (min)	95th percentile longest duration until a randomly assigned target can be tracked	0 ← 300
track life (min)	95th percentile shortest duration of continuous target monitoring	1 → 60
tracking latency (min)	95th percentile longest duration until Moving Target Identification data is received by warfighter	1 ← 240

Number of Target Boxes. The number of target boxes is defined as the number of 200x200 km target boxes that can be imaged by a single satellite during a single pass while maintaining the minimum required radar cross section and detectable velocity for a given target set. Figure 7-4 depicts the single-attribute utility function and weighting factor (k_i) for number of target boxes.

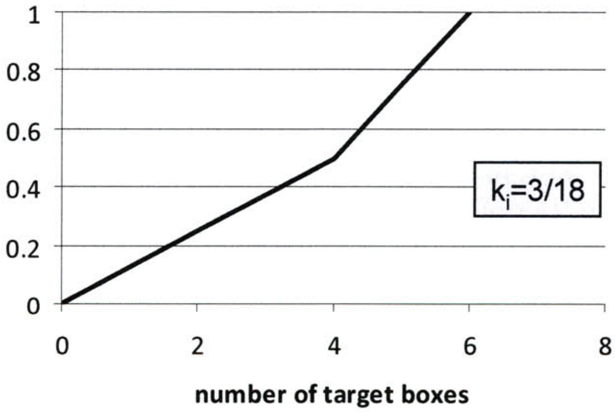


Figure 7-4. Utility for Number of Target Boxes

[42] The attributes are used to compute the utility using multi-attribute utility methods. Given the sensitive nature of precisely quantifying the military value proposition for satellite radar, the attribute ranges and utility functions are based on approximate data provided by the decision-maker. While conducting formal utility interviews are preferred for mapping the attributes to utility, these proxy values are better than assuming an objective function. In general, the attributes that range over many orders of magnitude are assumed to map logarithmically to the attributes, while attributes with narrower ranges have a more linear mapping. Although independently elicited, the attribute set maps closely to the attribute set used in a 2002 study of SBR alternatives by Lincoln Laboratories: tracking area, minimum detectable speed, SAR resolution, SAR area, geolocation accuracy, gap time, and center of gravity area (Spaulding 2003).

Minimum Detectable Velocity. MDV describes the lowest possible velocity of a target that can be detected from the backdrop of its surroundings. In order to determine this attribute, a minimum velocity allowed by physics is determined as a function of the transmit frequency, satellite velocity, and antenna size. This pure MDV assumes an object traveling directly below the satellite. In order to take into account the loss of tracking ability as a target moves farther towards the horizon, the cosine of the elevation angle is multiplied by pure MDV. Thus, the computed MDV is the best tracking possible for a target at a maximum viewable distance. A user would get a better minimum detectable velocity as the target moves within this boundary; however it is always assumed that the target is placed at the boundary. Figure 7-5 depicts the single-attribute utility function and weighting factor for MDV.

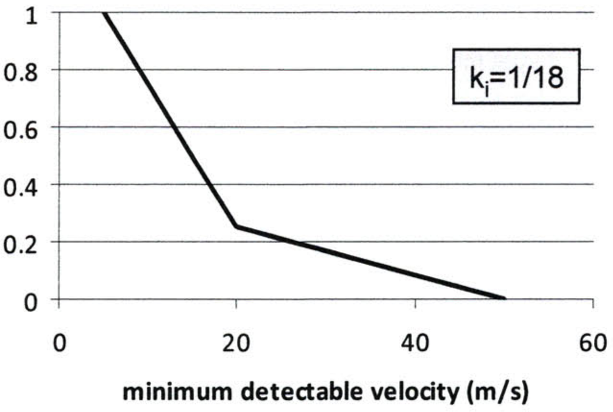


Figure 7-5. Utility for Minimum Detectable Target Velocity

Minimum Radar Cross Section. The cross section is defined as the minimal target area, in square meters, capable of reflecting a signal detectable by the radar's receiver in response to a radar pulse. The minimum RCS is calculated as a product of the range and azimuthal resolutions of targets at a fixed reflectivity, and therefore does not have to account for the backscattering coefficients of various surfaces and viewing angles. It therefore carries with it the tacit assumption that the satellite will dwell long enough to achieve parity in range and azimuthal resolutions. Figure 7-6 depicts the single-attribute utility function and weighting factor for minimum RCS.

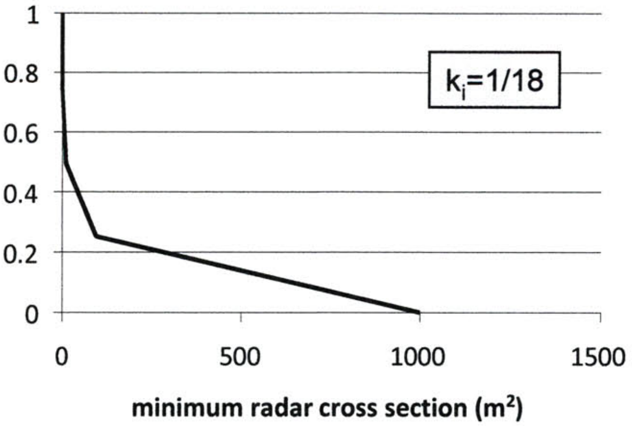


Figure 7-6. Utility for Minimum Radar Cross Section

Target Acquisition Time. Target acquisition time is the 95th percentile longest duration until a randomly assigned target (that can be tracked) is detected. Since gap lengths are probabilistic in nature, a 95th percentile is used to provide the effective worst case time. While the target acquisition time will generally be significantly lower than the computed time, this model outputs a time that will not only better reflect the variance in the systems, but will also provide users with a realistic idea of the maximum amount of time they may need to wait before acquiring an observation of a target. Figure 7-7 depicts the single-attribute utility function and weighting factor for target acquisition time.

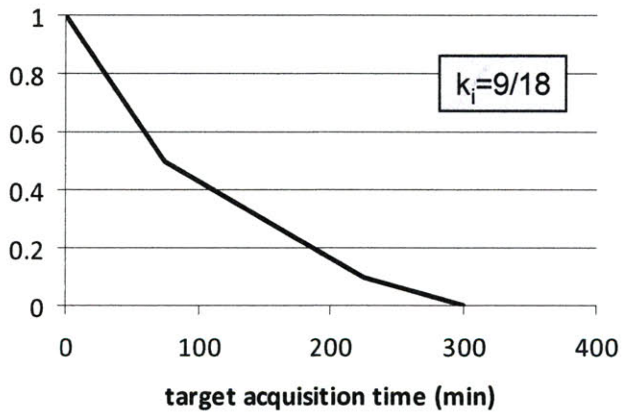


Figure 7-7. Utility for Target Acquisition Time

Target Track Life. Track life is the 95th percentile shortest duration that a target may be continuously monitored, where continuous observation is defined as an observation with no interruption lasting longer than a minute. Limiting the permitted interruption allows for satellites to work together to monitor a target. (In practice, this attribute is almost entirely a satellite-level rather than constellation-level attribute, given that the number of satellites necessary for assured global coverage from LEO is higher than the designs under consideration. Therefore, this attribute is largely an indicator of the size of the radar swath.) Figure 7-8 depicts the single-attribute utility function and weighting factor for target track life.

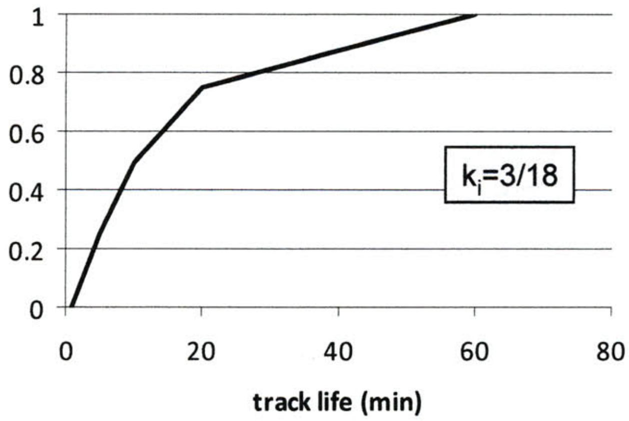


Figure 7-8. Utility for Track Life

Tracking Latency. The tracking latency is the 95th percentile longest delay between GMTI data collection on the space platform and the reception of GMTI data by the warfighter. Figure 7-9 depicts the single-attribute utility function and weighting factor for tracking latency.

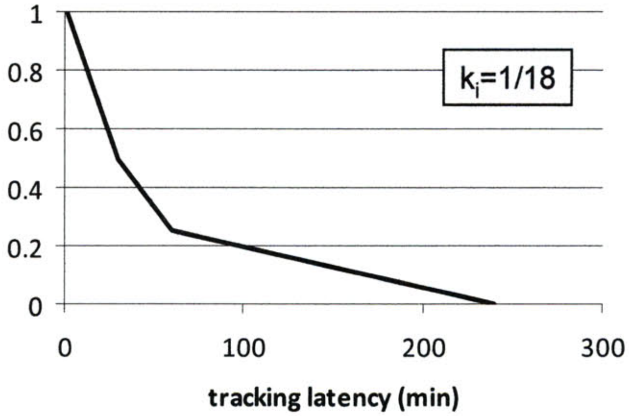


Figure 7-9. Utility for Tracking Latency

To determine the multi-attribute utility for the GMTI mission, a simple linear-weighted sum is used in which the single-attribute utilities are multiplied by their respective k_i weighting factors:

$$U(\underline{X}) = \sum_{i=1}^{6} k_i \cdot U(X_i) \qquad (7\text{-}2)$$

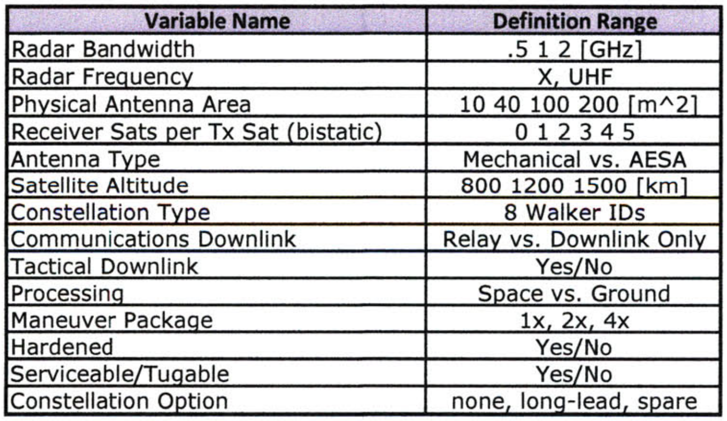
To incorporate survivability considerations into the value elicitation phase, it is necessary to consider whether stakeholder expectations change during and immediately after disturbance events. If this is the case, the acceptability ranges of the attributes comprising the utility function may be relaxed for short durations. In addition, it is also possible that the attribute set comprising the utility function will change. These changes are operationalized by characterizing stakeholder needs over time through a required value threshold (*i.e.*, zero utility in nominal environments), an emergency value threshold (*i.e.*, zero utility in perturbed environments), and a permitted recovery time (*i.e.*, allowable time before performance expectations return to nominal).

For the case of a constellation of military radar satellites, tactical user expectations for GMTI are unlikely to change as a function of localized disturbances from the natural space environment. In contrast to the space tug system that provides an infrastructure capability for infrequent servicing events, the satellite radar system is intended to support real-time operations. Assured access to the GMTI capability may be critical to the warfighter. Furthermore, as a military system, it is reasonable to consider disturbance events as part of the normal operating environment. Therefore, it is assumed that the required value threshold of the decision-maker is equivalent to the emergency value threshold (*i.e.*, V_x=V_e=0). Since expectations on the satellite radar are constant over the lifecycle, it is unnecessary to specify permitted recovery time.

7.2.2. Phase 2: Generate Concepts

Following elicitation of decision-maker attributes, the RSC development team generated several alternative design concepts for the satellite radar tradespace. The concepts generated were limited to conventional vehicles, and informed by existing analyses of military satellite radar (Post, Bennett and Hall 2006; CBO 2007; Pillai, Li and Himed 2008). Current or near-future SR technology documented in the literature (Davis 1999; Davis 2003) constrained the design space. It was assumed that satellite radar platforms are deployed in constellations to provide suitable coverage statistics. The satellites interact with existing or near-future space communication and ground communication infrastructure to disseminate GMTI data. Consideration was also given to the possibility of direct, in-theater tasking and downlink. Given these basic assumptions and general concept, a wide range of possible designs were enumerated based on the preliminary set of design variables (Table 7-4).

Table 7-4. Preliminary Design Variables for Satellite Radar



Variable Name	Definition Range
Radar Bandwidth	.5 1 2 [GHz]
Radar Frequency	X, UHF
Physical Antenna Area	10 40 100 200 [m^2]
Receiver Sats per Tx Sat (bistatic)	0 1 2 3 4 5
Antenna Type	Mechanical vs. AESA
Satellite Altitude	800 1200 1500 [km]
Constellation Type	8 Walker IDs
Communications Downlink	Relay vs. Downlink Only
Tactical Downlink	Yes/No
Processing	Space vs. Ground
Maneuver Package	1x, 2x, 4x
Hardened	Yes/No
Serviceable/Tugable	Yes/No
Constellation Option	none, long-lead, spare

The preliminary design vector in Table 7-4 includes elements of the radar sensor deployed, orbital properties of the satellite platforms, communications systems, and other satellite capabilities. Selecting a value for each particular design variable involves making a host of trade-offs. For example, as discussed by the Congressional Budget Office (2007), two major options exist for radar antennae: AESA or conventional reflectors. While the AESA design allows the radar beam to be steered electronically (and are also helpful for cancelling clutter and mitigating electronic jamming), the reflector is lighter and less expensive than an AESA. An example of an orbital trade is the selection of inclination angle: higher inclinations provide better access to polar regions but at the expense of equatorial areas.

Even before considering orbit and constellation trades, just the radar range equation (introduced in Section 7.1.1 without losses, L) provides a multi-dimensional tradespace.

$$R_{\max} = \sqrt[4]{\frac{P_t \cdot G^2 \cdot \lambda^2 \cdot \sigma}{P_{e_{\min}} \cdot (4\pi)^3 \cdot L}} \tag{7-3}$$

In selecting orbit altitude (*i.e.*, range), higher orbits are desirable as they provide better coverage of the Earth's surface and have lower velocities for GMTI. However, the wide-area surveillance rate for GMTI is proportional to the radar's power-aperture product and is inversely proportional to the square of the altitude (CBO 2007).

Increasing the transmitted power is desirable as it improves the signal-to-noise ratio at the receiver and helps to overcome signal propagation losses. However, increasing P_t also drives up satellite cost by increasing the mass required for energy production and storage. Similarly, increasing antenna gain is desirable for concentrating power on targets and increasing the reception area. Conversely, materials technology constraints may limit the deployment of large, light, deployable apertures.

Another tradeoff inherent in the radar range equation is the selection of radar frequency. While high-frequency wave forms enable higher-resolution radar images, they are also susceptible to atmospheric attenuation and other signal attenuation losses.

Having generated a parametric space that covers a wide range of possible designs (Table 7-4), the design variables are mapped to the attributes to ensure that the system concepts address the needs articulated by the decision-maker. Table 7-5 provides the design value mapping matrix for satellite radar, evaluating the importance of each preliminary design variable against attributes for GMTI, SAR imaging, and programmatic cost and schedule.[43] This mapping consists of a qualitative assessment following a modified Quality Function Deployment process (as documented in Section 6.2.3.)

[43] In applying RSC to satellite radar, the developed team focused on overall program utility, including attributes for GMTI, SAR imaging, cost, and schedule. The application of MATE for Survivability in this chapter uses a subset of the attribute analysis, focusing on the mission utility provided by GMTI.

Table 7-5. Design Value Mapping Matrix – Satellite Radar

			ATTRIBUTES															
			Mission											Programmatics				
			Tracking						Imaging					Cost		Schedule		
	Variable Name	Definition Range	Minimum Target RCS	Min. Detectable Velocity	Number of Target Boxes	Target Acquisition 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**
	Radar Frequency	X UHF	9	9	3	3	1	1	9	9	9	0	1	3	3	3	3	**66**
	Physical Antenna Area	10 40 100 200 [m^2]	9	9	9	3	1	1	9	9	9	1	1	9	9	9	9	**97**
	Receiver Sats per Tx Sat	0 1 2 3 4 5	9	9	3	3	1	1	9	3	3	1	1	9	9	9	9	**79**
	Antenna Type	Mechanical vs. AESA	9	9	9	3	3	1	9	9	9	1	1	9	9	9	9	**99**
	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**
	Processing	Space vs. Ground	0	0	0	1	0	3	1	0	0	0	3	9	9	9	9	**44**
	Maneuver Package	1x, 2x, 4x	1	1	1	1	1	0	1	1	1	1	0	9	3	3	3	**27**
	Tugable	Yes vs. No	1	1	1	1	1	0	1	1	1	1	0	9	9	9	9	**45**
	Constellation Option	none, long-lead, spare	0	0	0	0	0	0	0	0	0	0	0	9	9	9	9	**36**
	Total		65	64	42	39	30	33	66	58	62	23	33	106	100	88	100	

The design value mapping matrix helps to establish the design vector by indicating which design variables are of highest priority based on their total impact across the attributes (rows), and by ensuring that the selected design variables adequately drive value delivery across all of the decision-maker-derived attributes (columns).

Table 7-6 shows the baseline design vector established by the RSC development team. Several assumptions are implicit in the selected design vector, including the use of a monostatic radar architecture, circular orbits, and an AESA design. Despite these assumptions which limit the design space, a full-factorial sample of the enumerated design variables yields 23,328 candidate system designs. Although this is a very large number, particularly in comparison to the small number of alternatives analyzed in similar studies (CBO 2007), consideration of tens of thousands of designs is not impractical assuming that an efficient model can be developed.

Table 7-6. Baseline Design Vector – Satellite Radar

Design Variables	Steps	Enumerated Range	Units/Notes
Orbit Altitude	3	[800, 1200, 1500] *10^3	m
Walker ID Number	8	[1:8]	Walker Lookup Table
Radar transmit frequency	1	[10] *10^9	Hz
Antenna Area	3	[10,40,100]	m^2
Antenna Type	1	[0]	0=AESA, 1=Mech
Radar Bandwidth	3	[0.5,1,2] *10^9	Hz
Peak Transmit Power	3	[1.5,10,20]	kW
Communications Downlink	2	[0,1]	0=backbone, 1=ground
Tactical Downlink	2	[0,1]	0=yes, 1=no
Tugable	1	[1]	0=no, 1=yes
Maneuver Package	3	[4,5,6]	4=baseline, 5=baseline*2, 6=baseline*4
Constellation Option	3	[1:3]	1=nothing, 2=long lead parts, 3=spares built

7.2.3. Phase 3: Characterize Disturbance Environment

Once the baseline design vector is established, the next step in a traditional MATE study is to model the performance of the design alternatives to estimate lifecycle cost and utility. In MATE for Survivability, this step is preceded by two phases: characterizing the disturbance environment (Phase 3) and applying the survivability principles to the design vector (Phase 4).

Having selected a general system concept for the satellite radar system, environmental disturbances are enumerated and characterized. Table 7-7 shows the disturbances for an Earth-observing satellite operating at 800-1500 km and a 53° inclination. Since 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. The importance estimates for the first four disturbances in Table 7-7 are based on Pisacane (2008) and the subsequent estimates are based on engineering judgment. For example, aerodynamic drag forces from 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 7-7. Environmental Disturbances to Satellite Radar[44]

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 disturbances are checked for non-additive interactions. For example, an intelligent pairing of certain disturbances by an adversary may lead to non-linear losses in value delivery. Given an intelligent adversary, it would be necessary to include such combinations of disturbances as additional rows in Table 7-7.

For the analysis of satellite radar, the focus is on naturally occurring disturbances in the space environment that are assumed to be randomly distributed. Therefore, while it remains necessary to model the impact of extreme combinations of disturbances (*e.g.*, loss of communications relay coupled with global signal attenuation) in Phase 6, such interactions do not dominate the general characterization of the disturbance environment in Phase 3.

7.2.4. Phase 4: Apply Survivability Principles

Following enumeration of disturbances, the seventeen survivability design principles (Section 4.4) 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. Given the baseline set of design variables and environmental disturbances, a variety of concept enhancements may brainstormed for the satellite radar mission. The first two columns of the Survivability Design Variable Mapping Matrix (Table 7-8) illustrate this mapping. For example, the design principle of margin is 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 is also applied to different elements of the system architecture, including the satellite-level, constellation level, and ground segment. In all, 24 concepts are generated from 13 of the survivability design principles. (Given the focus on natural disturbances, the selected Type I survivability design principles that modify the observations, decision-making, and actions of hostile actors are not applicable).

[44] The importance score provides a relative ranking of disturbances in the space environment on mission impact. The scores may range from 0 (*i.e.*, effects produced can be ignored) to 10 (*i.e.*, effects produced will negate mission).

Table 7-8. Survivability Design Variable Mapping Matrix

				disturbances							
	design principles	concept enhancements	design variables (units)	atmospheric drag fluctuations	arc discharging	high-flux radiation	micrometeorites / debris	signal attenuation	change in target characteristics	failure of relay backbone	loss of tactical ground node
Type I	prevention	reduce exposed s/c area	antenna area (m^2)	9	0	3	9	0	0	0	0
	mobility										
	concealment										
	deterrence										
	preemption										
	avoidance	s/c maneuvering	ΔV (m/s)	9	0	3	1	0	0	0	0
			s/c servicing interface	9	0	1	1	0	0	0	0
		ground receiver maneuverability	mobile receiver	0	0	0	0	3	0	0	3
Type II	hardness	radiation-hardened electronics	hardening (cal/cm^2)	0	3	9	1	0	0	0	0
		bumper shielding	shield thickness (mm)	0	0	0	9	0	0	0	0
	redundancy	duplicate critical s/c functions	bus redundancy	0	1	9	3	0	0	0	0
		on-orbit satellite spares	extra s/c per orbital plan	0	1	3	3	0	3	0	0
		multiple ground receivers	ground infrastructure level	0	0	0	0	3	0	0	9
	margin	over-design power generation	peak transmit power (kW)	0	0	0	3	9	9	0	0
		over-design link budget	assumed signal loss (dB)	0	0	0	0	9	0	0	0
		over-design propulsion system	ΔV (m/s)	3	0	3	0	3	9	0	0
		excess on-board data storage	s/c data capacity (gbits)	0	0	0	0	0	0	3	3
		excess constellation capacity	number of satellites	0	1	3	9	0	0	0	0
	heterogeneity	interface with airborne assets	tactical downlink	3	3	3	3	3	3	3	3
		multiple communication paths	communications downlink	0	0	1	1	9	0	9	3
			tactical downlink	0	0	1	1	9	0	9	3
	distribution	spatial separation of spacecraft	orbital altitude (km)	1	1	3	3	0	9	0	0
		spatial separation of s/c orbits	number of planes	0	0	3	9	0	1	0	1
	failure mode reduction	reduce s/c complexity	bus redundancy	0	0	9	0	0	0	0	0
	fail-safe	autonomous operations	autonomous control	0	0	0	0	3	0	3	3
	evolution	flexible sensing operations	antenna type	0	0	0	0	3	9	0	0
			radar bandwidth (GHz)	0	0	0	0	9	3	0	0
		retraction of s/c appendages	reconfigurable	0	0	9	3	0	0	0	0
	containment	s/c fault monitoring and response	autonomous control	0	1	3	1	0	0	0	0
T III	replacement	rapid reconstitution	constellation spares	0	1	3	9	0	0	0	0
	repair	on-orbit-servicing	s/c servicing interface	9	1	3	3	0	3	0	0

The next step illustrated in Table 7-8 is to parameterize the survivable concepts by specifying 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. 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 final 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 (Table 7-5), 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 7-8, 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 in the link budget will reduce the impact of signal attenuation but will not directly mitigate any of the other disturbances.

Table 7-9 shows how the redundant design variables are consolidated and ordered to inform selection of the final 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 7-9 illustrate the output of this task for the satellite radar system.

Table 7-9. Selection of 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	atmosphenc 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		

Finally, the consolidated set of baseline and survivability design variables is examined to select a small number for inclusion in the tradespace. As illustrated in the "type" column in Table 7-9, many survivability design variables are already inherent in the baseline tradespace (*i.e.*, latent survivability trades).

Four considerations may be incorporated into the process of determining which dedicated survivability design variables to include. First, the coverage of the consolidated set of design variables across the seventeen design principles may be inspected (Table 7-9). 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.

Second, the mitigating impact of each consolidated design variable across the set of disturbances may be estimated by using a linear-weighted sum (in which weights are based on disturbance impact) (Table 7-7). In Table 7-9, the survivability design variables are ordered by this estimate of mitigating impact.

Third, it is important to consider downstream constraints associated with the modeling effort and computing resources when expanding the design-space. While it may be theoretically possible to parameterize all of the design principles and selectively sample the design-space using multi-disciplinary design optimization techniques (*e.g.*, genetic algorithms), such an implementation would require orders-of-magnitude increases in the modeling effort. While the geometric growth of the tradespace (as design variables are added) may be addressed by selectively sampling the tradespace or by gaining access to a super-computer, developing a stochastic, physics-based performance model for every disturbance and mitigating design variable is not a task that may offloaded to computers. Therefore, unless the system analyst has access to a team of engineers, there is a limit to how many survivability design variables may be incorporated into the final design vector.

Fourth, engineering judgment and knowledge gained from previous iterations of the MATE model may inform 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 four considerations, two additional survivability design variables were selected for inclusion in the satellite radar tradespace: constellation spares and shielding thickness.

Table 7-10. Finalized SR Design Vector (n=3888)

n=3888

Orbit Altitude (km)
800
1500

Walker ID
5/5/1
9/3/2
27/3/1
66/6/5

Antenna Area (m^2)
10
40
100

Peak Transmit Power (kW)
1.5
10
20

Radar Bandwidth (MHz)
500
1000
2000

Comm. Architecture
Direct Downlink Only
Relay Backbone

survivability variables

Constellation Spares
0
1
2

Shield Thickness (mm)
1
5
10

Table 7-10 provides the final design vector for satellite radar. As the independent variables for subsequent tradespace exploration, sampling these parameters is intended to define concepts that offer interesting trades among lifecycle cost, design utility, and survivability. Although two dedicated survivability design variables have been added to the final design vector, the 3888 possible combinations is less than the 23,328 possible combinations contained in the baseline design vector in Table 7-6. This reduction in the design space occurs because the number of steps has been reduced for orbit altitude and Walker ID number[45] while the tactical downlink and maneuver package design variables have been set to fixed values.

In this application of MATE for Survivability, it is possible to add survivability design variables while reducing the size of the overall design vector because the survivability analysis incorporates lessons learned from a previous iteration of static tradespace exploration.[46] In particular, knowledge of the tradespace generated by the baseline design vector and performance model informs setting some design variables to constants where obvious design decisions exist (*e.g.*, including tactical downlink). This downstream knowledge of the tradespace also informs the selection of enumeration steps and ranges (*e.g.*, halving candidate Walker constellations by fixing inclination at 53° while increasing average constellation size to improve coverage statistics). Reducing the size of the design vector is helpful for accelerating the computation of the static cost-utility tradespace in Phase 5, and crucial for the computationally-intensive modeling of utility trajectories in Phase 6.

7.2.5. Phase 5: Model Baseline System Performance

Following the completion of the concept and context generation activities, the RSC development team created an efficient, mid-fidelity computer model to determine the attribute, utility, and cost values for each design enumerated in the tradespace. To enable concurrent and collaborative model development, the satellite radar system was decomposed into several MATLAB modules to determine attribute values and intermediate variables given a design. The attribute outputs are then used to compute lifecycle cost and design utility.

Table 7-11 shows the software architecture for the satellite radar model. The model translates designs from the design vector in a given epoch and computes the corresponding costs, attributes, and utilities. In particular, each design of interest is enumerated, and then run through the modules sequentially by a main loop, which stores the computed values for each design for subsequent exploration and analysis. As evidenced by the lack of above-diagonal dependencies in Table 7-11, the modules are carefully structured such that they can be executed sequentially without iteration or optimization loops. Eliminating feedback among modules is critical for achieving reasonable runtimes (of a few minutes) on current desktop computers.

[45] The Walker notation is used to describe symmetrical constellations of satellites in circular orbits. The three numbers refer to the number of satellites, the number of orbital planes, and the phasing of satellites in adjacent planes, respectively.

[46] The MATE for Survivability study of satellite radar followed the application of the baseline MATE process to satellite radar by the RSC development team.

Table 7-11. N^2 Diagram of Software Architecture for Satellite Radar

	Design Enumerator	Constants	Design Space Selector	Target	Orbit	Radar	Constellation	On-Board Processor	Communications	Ground Processor	Satellite Bus	Attributes	Cost	Utility	Survivability
Design Enumerator	■														
Constants		■													
Design Space Selector	X		■												
Target		X		■											
Orbit		X	X		■										
Radar		X	X	X	X	■									
Constellation		X	X	X	X	X	■								
On-Board Processor		X			X	X		■							
Communications		X	X		X	X	X	X	■						
Ground Processor		X								■					
Satellite Bus		X	X		X			X	X		■				
Attributes		X	X			X	X	X	X	X	X	■			
Cost		X	X			X		X	X	X	X		■		
Utility												X		■	
Survivability		X	X				X				X	X		X	■

The following paragraphs briefly describe the key computations performed by the individual modules. Given finite project resources, modules are written at an intermediate level of fidelity. Direct physics-based models are used where possible, and simplifying assumptions and heuristics are applied for less sensitive parts of the analysis.

Design Enumerator. Given the design variables (Table 7-10), the design enumerator creates a list of candidate designs through a series of nested "for" loops. Each design is numbered sequentially and stored.

Constants. The constants module returns a data structure containing fixed values regarding technology availability (*e.g.*, specific performance of solar array), modeling assumptions (*e.g.*, diameter of tactical downlink dish), and parametric cost estimating relationships. These constants span the payload, processing, communications, and bus subsystems. In the development of RSC, modeling activities involved creating a unique static tradespace for each enumerated epoch context (Table 7-2). As each epoch is defined by varying constants in the epoch vector, many of the constants become variables in RSC. In contrast, in the application of MATE for Survivability, a single static tradespace is computed given a fixed set of constants representing a nominal epoch context. The nominal context is based on the availability of technology with technology readiness level (TRL) 9 or higher, current generation launch vehicles, and a communications infrastructure based on DoD's Wideband Global SATCOM System (WGS) and the Air Force Satellite Control Network (AFSCN). Communications jamming is turned off in the computation of baseline system performance.

Design Space Selector. The design space selector takes a sample of enumerated designs. In this case application, a full-factorial sample is selected, including all 3,888 possible combinations of the eight design variables.

Target. The target module selects a target set from the list of targets elicited from subject matter experts. The target is characterized by a constant array of structures, each containing target location, RCS, velocity, and terrain type. Terrain type is operationalized as minimum elevation angle. For the baseline system performance, the target set is based on an operations plan which distributes large moving targets in East Asia and small moving targets in the Middle East.

Orbit. The orbit module computes basic orbital properties that are required inputs to the radar module. Given an orbital altitude and Walker formation, orbit radius, satellite velocity, maximum eclipse length, and orbit period are computed using basic geometry. A circular orbit and a spherical earth are assumed, as well as constant satellite altitude and velocity.

Radar. The radar module computes the performance attributes of the radar specified by the design variables as a function of the calculated orbit and given target deck. Computation of the radar attributes is complicated because the attributes can be traded against one another. To decouple these computations, a major assumption of the CONOPS is that evaluation of particular attribute occurs when the radar is operating in such a way as to optimize that attribute.[47] For example, the minimum detectable RCS is computed by assuming a dwell time long enough to achieve the maximum theoretical performance by the given bandwidth and dimensions of the radar system. However, when evaluating the number of target boxes, the sensor dwells on each target only for the duration necessary for detection before advancing to the next target area. Therefore, most radar systems evaluated achieve good minimum RCS while the average number of target boxes is the attribute most sensitive to the traditional radar performance metrics of antenna area and power. While not realistic in practice, such assumptions are reasonable for evaluation purposes (*e.g.*, had dwell time been fixed, minimum RCS would have become sensitive to antenna area and power).

Given these simplifying assumptions, the radar module uses basic geometry and physics to calculate several intermediate variables and the desired performance attributes (Wertz and Larson 1999). The module is decomposed into twelve sub-modules. First, given the antenna area design variable, the length and width of the AESA is computed assuming a 4:1 length to width ratio. Second, beamwidth is estimated given the antenna area and transmit frequency and decibel value for transmitted signals. Third, the minimum detectable velocity is computed by calculating the pure MDV (as a function of the radar and satellite velocity) and then adjusting for the curvature of the Earth. (The MDV assumes that at some point the target of interest is travelling along the range direction towards the satellite in a vector parallel to the tangent plane of the earth at the sub-satellite point.) Fourth, the minimum and maximum elevation angles are determined by using the pure MDV to find the largest angle at which targets with the slowest velocity in the target deck are still detectable. Fifth, the distances from the satellite to the earth are computed when looking along the minimum and maximum elevation angles. Sixth, the radar

[47] By nature, AESA radars are flexible systems open to a wide variety of CONOPS. Rather than modeling the optimal CONOPS at all times in the simulation (outside of the study's scope) or including different CONOPS in the design vector (computationally prohibitive), this assumption makes the performance modeling tractable.

swath width is calculated using the range, signal wavelength, antenna width, and minimum elevation angle. Seventh, the angular difference of the leading and trailing radar beams from the center of the Earth is estimated at the subsatellite point. Eighth, the duty cycle is found as the product of pulse repetition frequency and pulse width. Ninth, the average power utilization of the radar is calculated given the design variable of peak transmit power, duty cycle, and transmit efficiency. Tenth, the antenna gain is computed as a function of antenna diameter, transmit efficiency, and frequency. Eleventh, the unattenuated range resolution of the satellite is computed as a function of beamwidth and gain, given the speed of light and assuming a constant noise value. Twelfth, the time per target per beam to achieve an acceptable signal to noise ratio is computed and used to determine the amount of time needed to dwell on a target to get sufficient RCS resolution. Finally, the radar module applies the calculated performance attributes to the radar range equation to check for errors.

Constellation. The constellation module inputs the calculated radar performance attributes and orbit values and outputs coverage statistics and communications availability. Coverage statics are also pre-computed for cases involving the random loss of one or more satellites. The constellation module uses the time and altitude data from the orbit module to simulate satellite movement on a minute by minute basis, projecting the surface area that each satellite can cover in each minute using the swath information from the radar module. An iterative simulation tracks the relative position and motion of targets, satellites, communications systems, and warfighter users of the GMTI data.

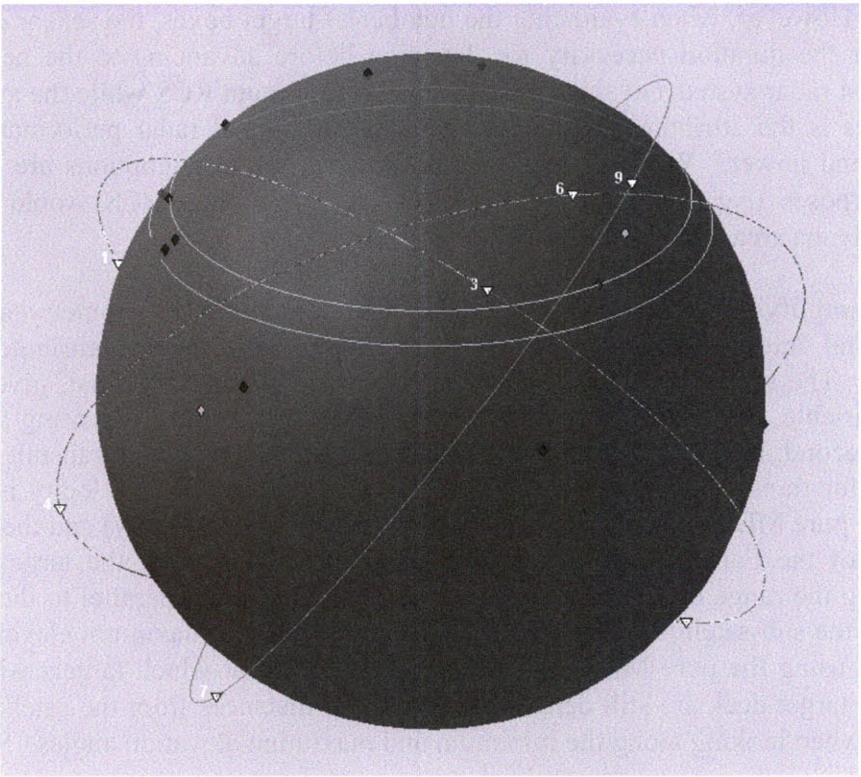


Figure 7-10. Visualization of SR Constellation Module

The computed coverage statistics match outputs in similar evaluations of satellite radar alternatives (CBO 2007). A dynamic visualization of satellite look-angles for target detection and communications (Figure 7-10) further validates the constellation module.

On-Board Processor. Taking inputs from the constants, orbit, and radar modules, the on-board processor module estimates the latency increment as well as the raw sensor data rate of the payload. Processor mass, cost, and power requirements are also computed.

Communications. The communications module estimates the data latency and the data throughput attributes as well as the mass, power, and cost of the spacecraft communications architecture. With inputs from the constants, design space selector, orbit, radar, constellation, and on-board processor modules, communications requirements and performance are determined using a link budget (Pratt, Bostian and Allnutt 2003). Given an input data rate from the radar module and downlink opportunities from the constellation module (assuming a 95th percentile worst case time between in view downlink locations), required compression and transmission rates are determined. (A data storage system is also sized for the direct downlink architecture.) These requirements are used to determine power requirements for an acceptable signal-to-noise ratio. As certain power requirements are unreasonable, the code selects among multiple satellite dish diameters in order to compensate for large data rates.

There are two communications architectures in the tradespace: direct downlink and relay backbone. For direct downlink, the downlink availability times multiplied by a latency factor determines the required downlink data rate. This downlink data rate is sent to the link budget to determine the mass, power, and cost of the communications system. For relay backbone, the downlink data rate is set by the capability of the system being utilized (e.g., WGS). The backbones are assumed to always be in view rather than a direct downlink which requires the satellite to be in view of a ground station.

Ground Processor. The ground processor module sets the latency associated with processing the data received from the constellation before it is received by the warfighter. As with other subsystem modules, recurring and non-recurring engineering costs are estimated.

Satellite Bus. The satellite bus module determines the spacecraft characteristics necessary to support the radar payload and communications system. First-order models of satellite structure, power, and propulsion subsystems are applied as well as heuristic measures for the attitude control and thermal control subsystems. The satellite bus module outputs the mass and cost of each satellite in the constellation.

Structural requirements are based on a panel-beam model of the deployed radar plane (designed to a stiffness criterion) and a simple mass-fraction model of the bus. The power subsystem is sized by integrating the power requirements of the other subsystems and calculating the mass of the solar array required to produce that power and the batteries needed for storage (at end-of-life). Propulsion requirements are determined by calculating the amount of propellant used throughout the spacecraft's lifetime, including maneuvers.

The satellite bus module also determines the U.S. launch vehicle and U.S. launch site for the satellites. Given orbit altitude, inclination, and Walker constellation type, the launch sub-module uses the assumptions in Table 7-12 (Isakowitz, Hopkins and Hopkins 2004) to select the least expensive vehicle that can be used, its launch cost, the available launch site, and the maximum number of satellites that may be launched by each vehicle.

Table 7-12. Launch Vehicle Assumptions in SR Model

Vehicle	*Payload to LEO*	*Launch Cost k$*	*Launches per year*	
			Cape Canaveral	*Vandenberg*
Atlas V 400	12,500 kg	75000	12	n/a
Delta IV Medium+	13,327 kg	116500	17	9
Atlas V 500	20,520 kg	110000	12	n/a
Delta IV Heavy	23,260 kg	154000	17	9
Ares I	24,453 kg	400000	4	n/a
Ares V	145,000 kg	1000000	1	n/a

Attributes. The attributes module takes the attributes calculated by the subsystem modules and wraps them in a single structure. It also computes attributes that are simple functions of intermediate variables from separate modules (*e.g.*, adding processing and communications latencies for tracking latency).

Cost. The cost module collects the non-recurring and recurring engineering cost estimates from the satellite subsystem modules to calculate the cost of an individual satellite and to estimate a baseline program lifecycle cost. Finally, an overall program lifecycle cost is computed based on the constellation sparing strategy.

Utility. Given outputs from the attribute module and the utility functions elicited from the decision-maker in Section 7.2.1, the utility module calculates the single-attribute utilities and the multi-attribute utility for each design alternative.

Survivability. Once the costs and benefits of design alternatives in a static context have been determined by calculating overall lifecycle cost and multi-attribute utility, the survivability module examines the performance of design alternatives in dynamic operational environments. The survivability module and its associated outputs are the subject of Section 7.2.6.

Having provided an overview of the satellite radar model, the remainder of this section describes the output of the static tradespace analysis. The baseline tradespace consisting of lifecycle cost and design utility is introduced, and the effect of each design variable on the tradespace is examined.

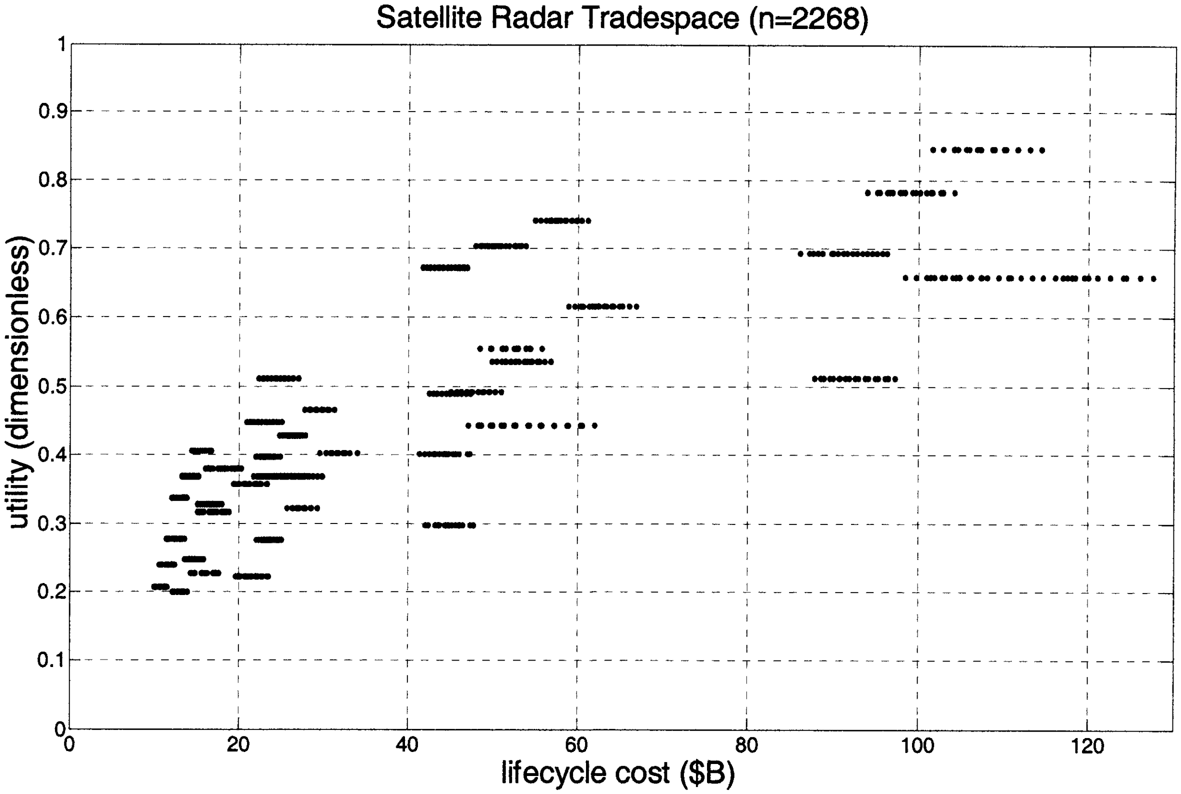


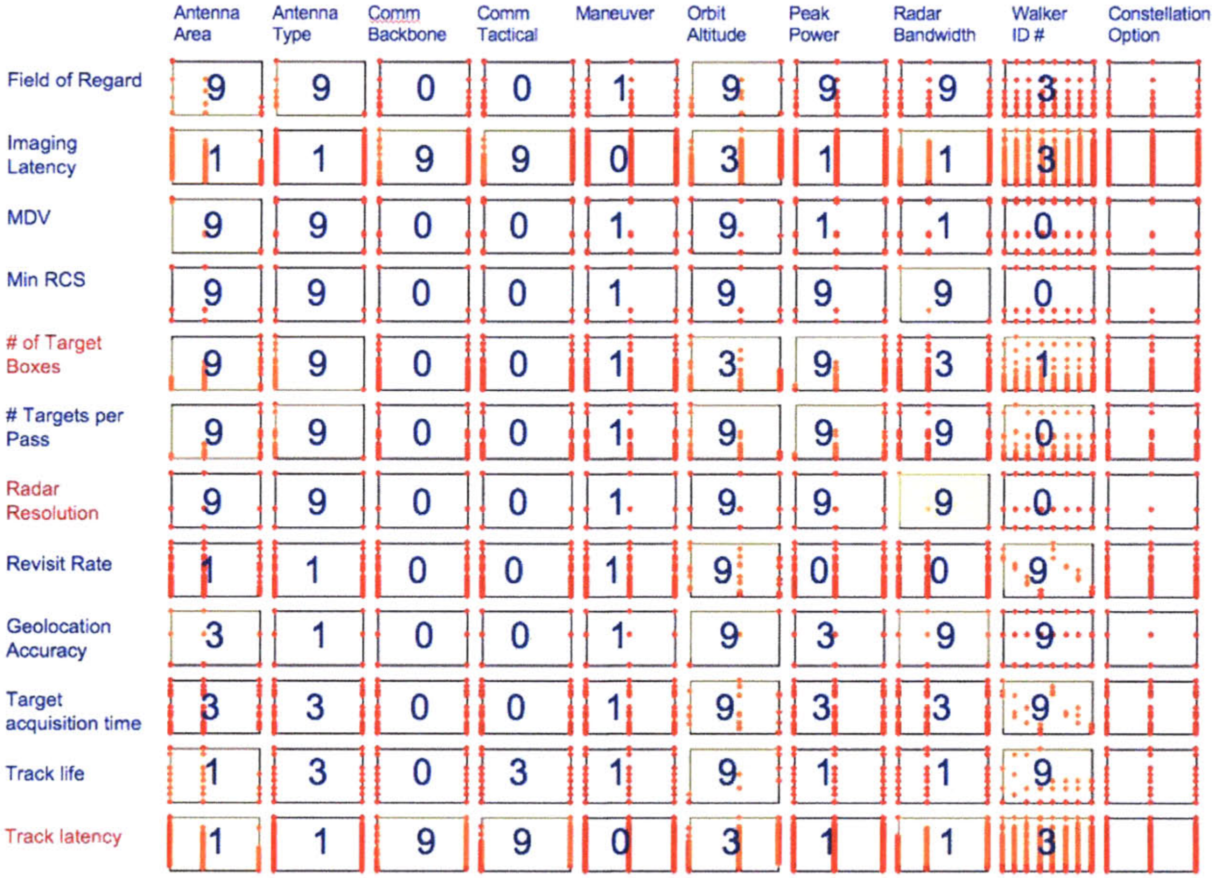
Figure 7-11. Baseline SR Tradespace

Figure 7-11 shows the baseline SR tradespace which evaluates each design alternative in a static, nominal environment. Each point represents a unique system architecture and is plotted in terms of a twenty-year lifecycle cost (in billions of dollars) and multi-attribute utility (as defined in Section 7.2.1). While 3888 design alternatives are generated from a full-factorial sampling of the design variables (Table 7-10), only 2268 are plotted in Figure 7-11 for consideration. This 42% reduction of the tradespace occurs because many of the designs fail to perform above the minimum acceptable level in one or more attributes. For example, the constellations composed of satellites with an antenna area of 10 m^2 are filtered from the tradespace (see Figure 9-11 in Appendix F).

The baseline tradespace includes 198 cost-utility Pareto-optimal designs (*i.e.*, designs of highest utility at a given cost). Within this set, the baseline tradespace reveals interesting trade-offs among Walker constellation type, antenna area, peak transmit power, and cost. Several different satellite radar constellations occupy different regions of the Pareto front, including sparse constellations with low power-aperture products, and dense constellations with greater transmit powers and antenna areas. In a simple MATE analysis, promising designs identified in the baseline tradespace (*e.g.*, designs on the "knee" of the Pareto front) might be selected for further evaluation.

To verify that the model outputs reasonable results, a sensitivity analysis is conducted on the relationship between the input design variables and output attribute performance levels. In

Figure 7-12, each box plots the sensitivity of an attribute (row) to a design variable (column). As the design variables are discrete, the plots are a series of lines, and differences in these lines indicate sensitivity (highlighted by shading). Accordingly, Figure 7-12 is similar to the design value mapping matrix in Table 7-5, but the results shown are from a physics-based model, not a set of assumptions and expert opinion. The numbers from the design value mapping matrix are overlaid on each plot, and a comparison is made. Most sensitivities behave as expected, validating the engineering judgment during concept generation.



	Antenna Area	Antenna Type	Comm Backbone	Comm Tactical	Maneuver	Orbit Altitude	Peak Power	Radar Bandwidth	Walker ID #	Constellation Option
Field of Regard	9	9	0	0	1	9	9	9	3	
Imaging Latency	1	1	9	9	0	3	1	1	3	
MDV	9	9	0	0	1	9	1	1	0	
Min RCS	9	9	0	0	1	9	9	9	0	
# of Target Boxes	9	9	0	0	1	3	9	3	1	
# Targets per Pass	9	9	0	0	1	9	9	9	0	
Radar Resolution	9	9	0	0	1	9	9	9	0	
Revisit Rate	1	1	0	0	1	9	0	0	9	
Geolocation Accuracy	3	1	0	0	1	9	3	9	9	
Target acquisition time	3	3	0	0	1	9	3	3	9	
Track life	1	3	0	3	1	9	1	1	9	
Track latency	1	1	9	9	0	3	1	1	3	

Figure 7-12. Design Vector to Attribute Sensitivity Study

To provide insights into engineering trades and interpret the results of the static analysis, a sensitivity analysis is also performed for each design variable on the baseline tradespace. In particular, a third dimension is added to the tradespace (*i.e.*, shape) to examine the overall effect of each design variable on cost and utility.

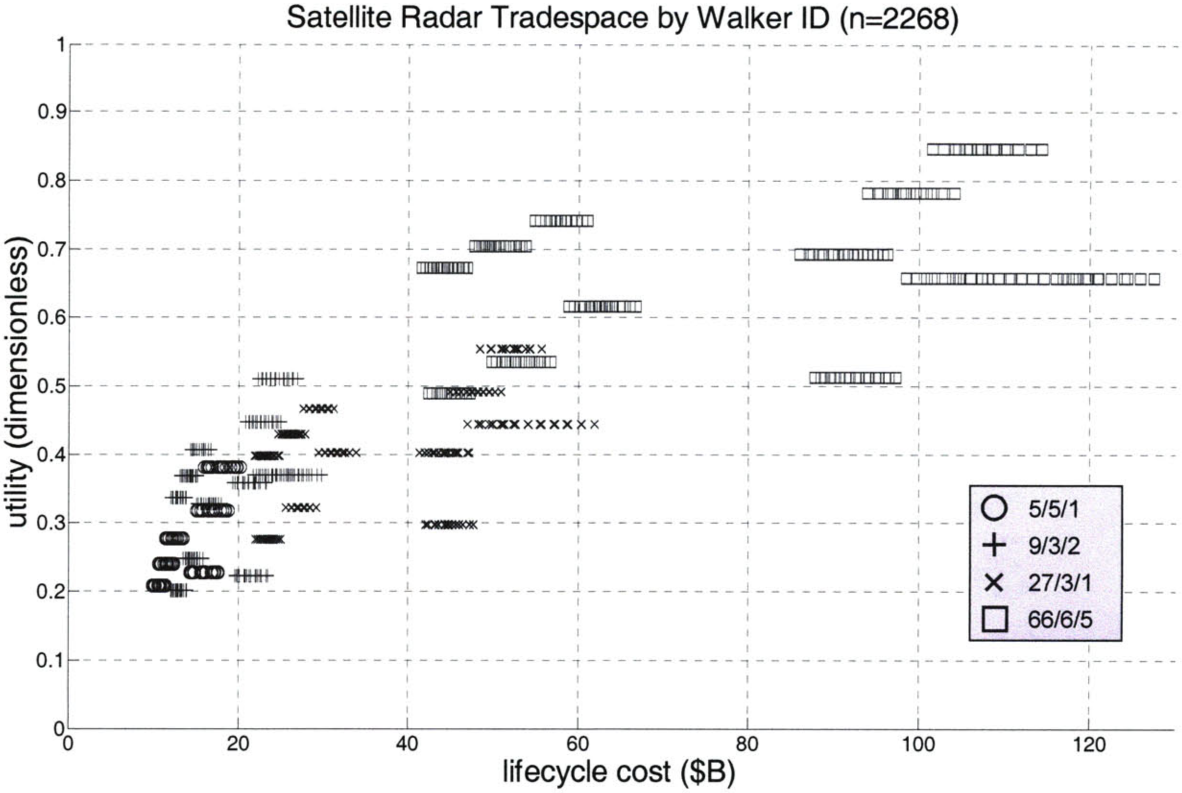


Figure 7-13. Effect of Walker Constellation on Baseline SR Tradespace

Figure 7-13 shows the effect of the Walker constellation design variable on the tradespace. The horizontal and vertical axes of the baseline tradespace are preserved to indicate lifecycle cost and utility, respectively. The dots in Figure 7-11 are replaced with shapes to indicate Walker constellation type. Examining the Pareto front in Figure 7-13 shows a direct correlation of constellation size with cost and utility. While sparse, five-satellite constellations occupy the lower-left of the tradespace, denser constellations dominate the upper-region region of greater cost and utility. This is an intuitive result as the denser constellations perform better in the attribute of target acquisition time. The larger constellations also have the potential to perform well in the attribute of target track life by handing-off tracks to successive satellites.

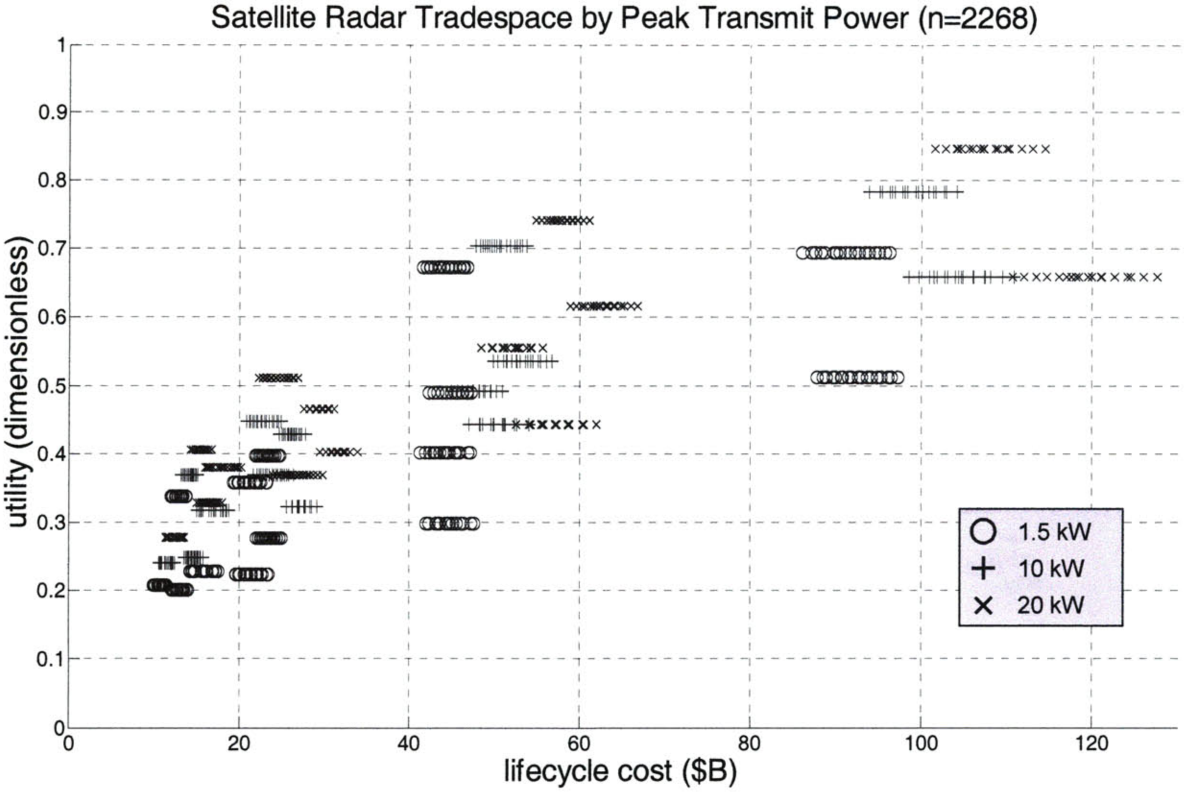


Figure 7-14. Effect of Peak Transmit Power on Baseline SR Tradespace

Figure 7-14 examines the effect of peak transmit power on the tradespace. As expected, low power systems dominate the lower performance, less-costly region of the Pareto front and higher power systems comprise the high performance region. The effect is not uniform as Pareto-efficient antennae with 20 kW of peak transmit power may deliver less utility than lower-powered systems due to the impact of antenna area. (The effect of antenna area, in addition to the effect of orbit altitude, radar bandwidth, and communications architecture, may be observed in the figures of Appendix F.) Ultimately, however, if one limits the search of the tradespace to the Pareto efficient region, power-aperture product becomes a clear trade between cost and performance.

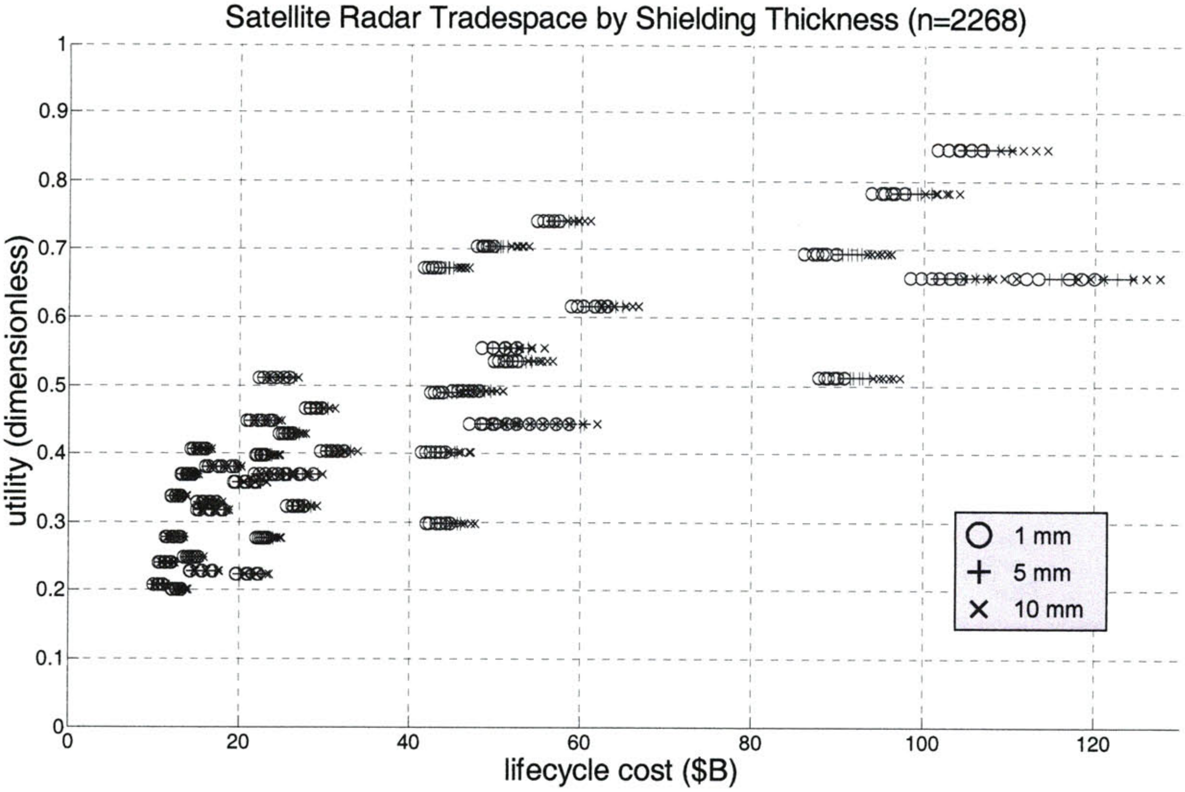


Figure 7-15. Effect of Shielding Thickness on Baseline SR Tradespace

Moving on to the dedicated survivability variables in the design vector, Figure 7-15 shows the effect of shielding thickness on the baseline SR tradespace. Interestingly, every design comprising the 198-count Pareto set incorporates the minimum shielding thickness of 1 mm. As demonstrated previously in the space tug computer experiments, the mitigating impact of survivability enhancement features on environmental disturbances is not accounted for in the static tradespace. In contrast to the previous space tug experiments, there is no utility loss associated with shielding because loss of ΔV from the mass penalty does not impact the attributes of satellite radar. However, the mass penalty of increasing shielding to 5 mm or 10 mm adds lifecycle cost (as a function of the exposed cross sectional area being shielded). As a result, all designs with increased shielding are in the interior region of the tradespace.

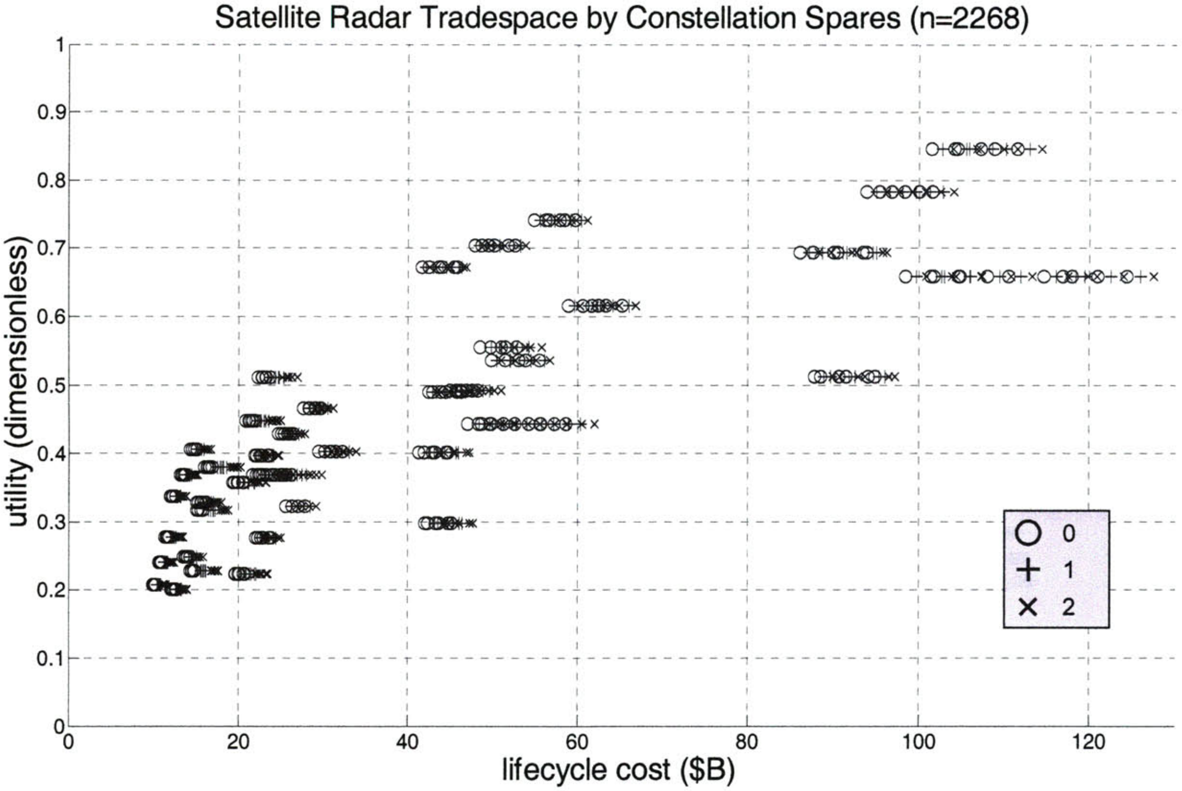


Figure 7-16. Effect of Constellation Spares on Baseline SR Tradespace

Figure 7-16 shows the effect of constellation spares on the baseline SR tradespace. As with shielding thickness, no designs incorporating this survivability design variable (*i.e.*, choosing to have at least one or two constellation spares for unplanned attrition) are included in the set of Pareto-optimal designs. Again, this is because purchasing spare satellites adds cost (*i.e.*, typically over $1B) without an impact on the utility of the system at beginning-of-life.

The subsequent section describes how the static tradespace analysis of satellite radar is extended to incorporate survivability considerations over the entire lifecycle.

7.2.6. Phase 6: Model Impact of Disturbances on Performance

Having calculated the lifecycle cost and beginning-of-life utility for each design alternative, the survivability module examines the performance of design alternatives in dynamic operational environments. The occurrence of uncertain future disturbance events from the natural space environment is modeled in a stochastic simulation, and a Monte Carlo analysis is conducted to extract representative distributions of utility trajectories. Two disturbances are incorporated into the analysis: micrometeorites/debris impacts and signal attenuation.

As an extension of the baseline MATE analysis, the survivability module is the final element of the SR software architecture. As shown in Table 7-11, the module receives inputs from the constants vector (*e.g.*, bumper shielding materials), design space selector (*e.g.*, shield thickness), constellation module (*e.g.*, pre-computed coverage statistics for degraded constellations), satellite bus module (*e.g.*, exposed cross-sectional area), and attributes and utility modules. These inputs are then used to model the susceptibility, vulnerability, and resilience of design alternatives. The output of an individual run of the model is a dynamic characterization of the system performance in the attributes. This dynamic characterization is translated to a multi-attribute utility trajectory for ten years of operational life. Since the simulation is path-dependent and stochastic, 500 Monte Carlo trials are conducted for each satellite radar constellation in the design vector.

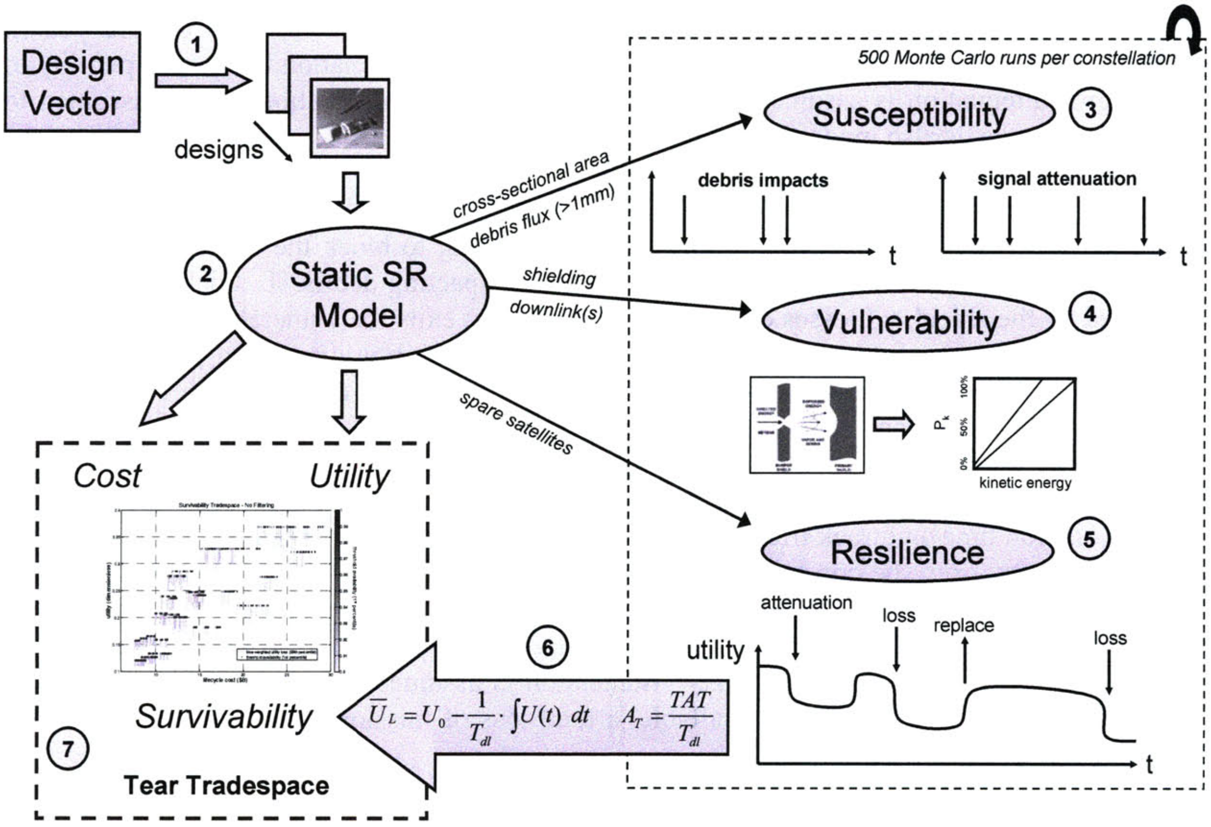


Figure 7-17. Incorporation of Survivability Considerations into Satellite Radar Tradespace

Figure 7-17 provides a flow-chart representation of how survivability considerations are incorporated into the satellite radar tradespace. Treating the baseline MATE model as a black-box, implementation of the survivability analysis involves seven general steps. First, the design vector is expanded to include survivability design variables (Table 7-10), including the addition of three levels of satellite shielding and the option to purchase up to two spare spacecraft to enable rapid reconstitution of the constellation. Taking a full-factorial sample of the design vector, this expansion grows the design space by a factor of nine. Second, the baseline MATE model of satellite radar is run to assess the performance of the expanded set of design alternatives. Accounting for the added cost and weight of shielding as well as the added cost of purchasing extra spacecraft, the attributes are recomputed followed by the calculation of total lifecycle cost and design utility. The preceding Section 7.2.5 shows the output of this static analysis.

In the following three steps, constellation health is modeled using a probabilistic simulation. In the third step, susceptibility to debris impacts is modeled as a function of the exposed cross-sectional area of alternative constellations and a typical debris flux for Earth-observation satellites. Debris event times, defined as an impact by an object >1 mm, are randomly generated according to a Poisson process (with the Poisson parameter set to the average inter-arrival time of historical debris flux) (Wiedemann et al. 2008). Given a debris event, the type of impact is determined by probabilistically sampling the distribution of debris sizes and assuming a fixed relative velocity of 7.5 km/s. Susceptibility to global signal attenuation is also modeled in the third step using Poisson arrivals (and assuming an average inter-arrival time of five years). Whereas susceptibility to debris varies by satellite design and constellation type, susceptibility to global signal attenuation is assumed uniform. The duration of attenuation events, assumed to average six months, is also modeled using the Poisson distribution.

In the fourth step, the vulnerability of the designs to the generated disturbances is assessed. In the case of debris events, the ability of the satellite shielding to block the debris is determined based on the shield thickness and the momentum of the impacting debris. If a debris impact can be repelled by the shield, no losses occur and the simulation exits the vulnerability model. If the shield is not thick enough to repel the debris, satellite vulnerability is assessed probabilistically using conservative assumptions from a binary loss model (*i.e.*, curve one in Figure 7-18). Taken from the literature (Wiedemann, Oswald et al. 2008), the empirically-derived loss model is based on the kinetic energy of the debris. If satellite failure occurs, the impact on constellation performance is determined by re-computing multi-attribute utility. In particular, the values of target acquisition time and track life for the degraded constellation are found using pre-computed coverage statistics from the constellation module. These attribute levels are used to recalculate the single-attribute utilities and overall multi-attribute utilities at the time of the debris impact. In the case of signal attenuation, vulnerability is based simply on the availability of a relay backbone for downlink communications. Attenuation is assumed to have no impact if such a backbone exists. If no backbone is available, a total loss of mission utility is assumed for the duration of the attenuation event.

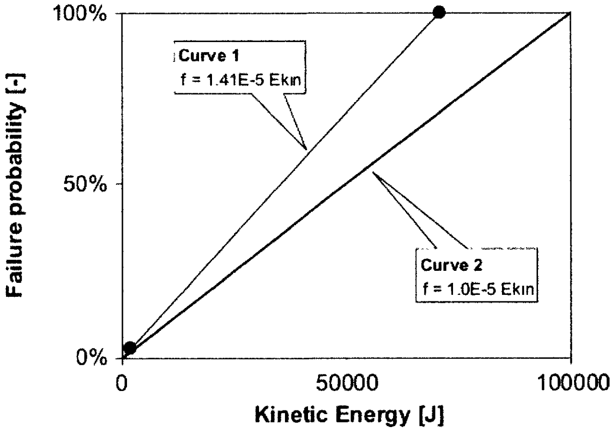
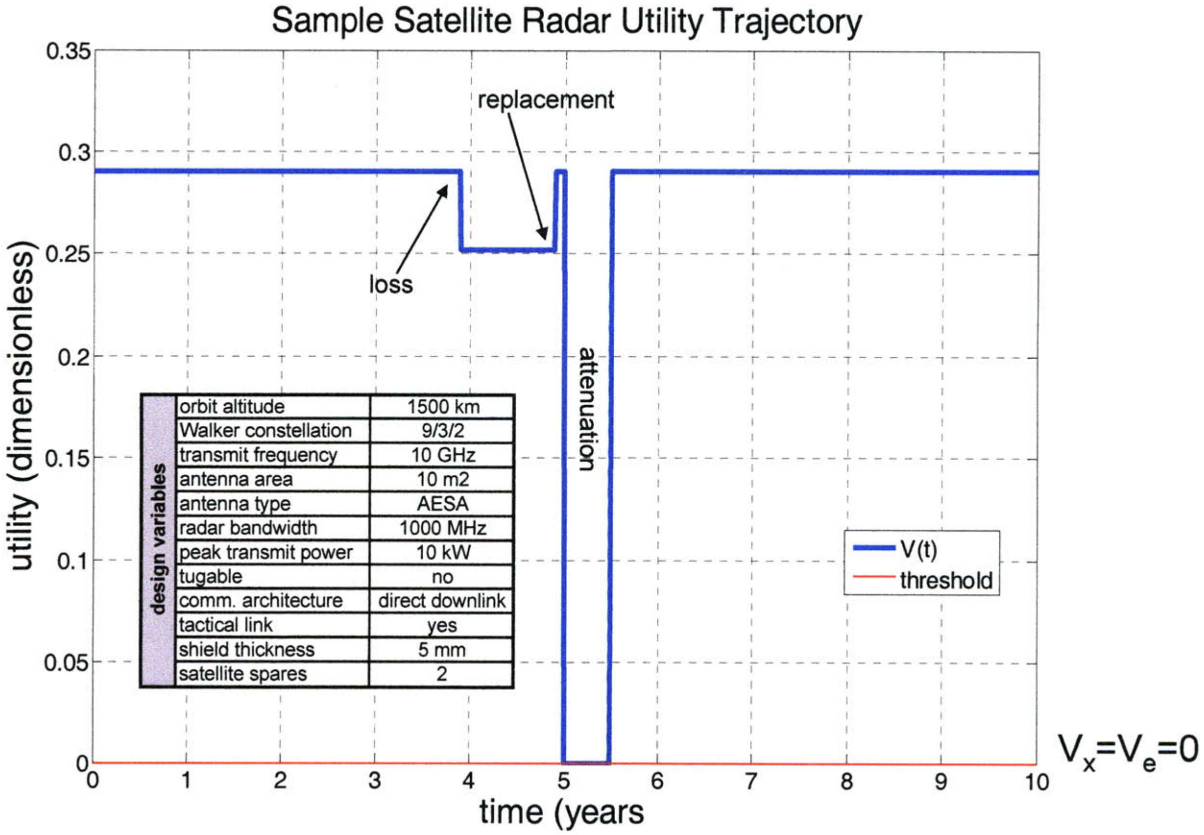


Figure 7-18. Failure Probability as a Function of Impact Kinetic Energy (Wiedemann, Oswald et al. 2008)

In the fifth step, the resilience of each design is assessed. If the output of the vulnerability model is a satellite loss, the design vector is checked for the availability of spare satellites. If a spare is available, a replacement satellite is launched. (Once launched, ground spares are not replaced.) The time of launch is assumed to be six months plus a random delay (according to a Poisson process with an expected value of six months). At the time of satellite replacement, the attribute levels and utilities are recomputed for the constellation. By continuously monitoring constellation performance in the attributes, multi-attribute utility may be assessed over the entire lifecycle. This dynamic characterization of overall system health is termed a utility trajectory. Figure 7-19 shows a sample utility trajectory, showing the impact of satellite loss, satellite replacement, and signal attenuation (in the absence of a relay backbone) on constellation performance. As discussed in Section 7.2.1, the required value threshold of the decision-maker is equivalent to the emergency value threshold (*i.e.*, V_x=V_e=0).



design variables	orbit altitude	1500 km
	Walker constellation	9/3/2
	transmit frequency	10 GHz
	antenna area	10 m2
	antenna type	AESA
	radar bandwidth	1000 MHz
	peak transmit power	10 kW
	tugable	no
	comm. architecture	direct downlink
	tactical link	yes
	shield thickness	5 mm
	satellite spares	2

Figure 7-19. Utility Trajectory Output from a Single Run of the Simulation

In the sixth step, time-weighted average utility and threshold availability are calculated at the end of each ten-year simulation as summary statistics for the utility trajectory output. As each run of the simulation is stochastic and path-dependent, a 500-run Monte Carlo analysis is performed for each design to obtain a significant sample of utility trajectories. In the seventh step, the probabilistic survivability metrics are integrated with the deterministic metrics of lifecycle cost and design utility for integrated tradespace exploration. These final two steps, application of the survivability metrics and tradespace exploration, are described in detail in the following two subsections.

7.2.7. Phase 7: Apply Survivability Metrics

Having modeled the impact of disturbances on the lifecycle performance of the design alternatives, the survivability metrics are applied to the utility trajectory outputs. Applying the survivability metrics requires establishing a percentile reporting level for the distribution of each metric.

Figure 7-20 depicts the distributions of time-weighted average utility achieved by 20% of the design alternatives over 500 Monte Carlo runs. (A random sample of 20% was selected to aid in information visualization.) Each column of points represents the distribution of time-weighted average utility for a single satellite radar design vector. (Figure 7-21 shows a histogram for one of these distributions.) To organize the data, the columns are ordered along the horizontal axis in terms of design utility—the deterministic beginning-of-life utility achieved by a constellation before stochastic losses accrue from disturbance events. The design utility here is equivalent to the utility axis in the baseline tradespace (Figure 7-11). A 45° line is also drawn to show the maximum time-weighted average utility value achievable.

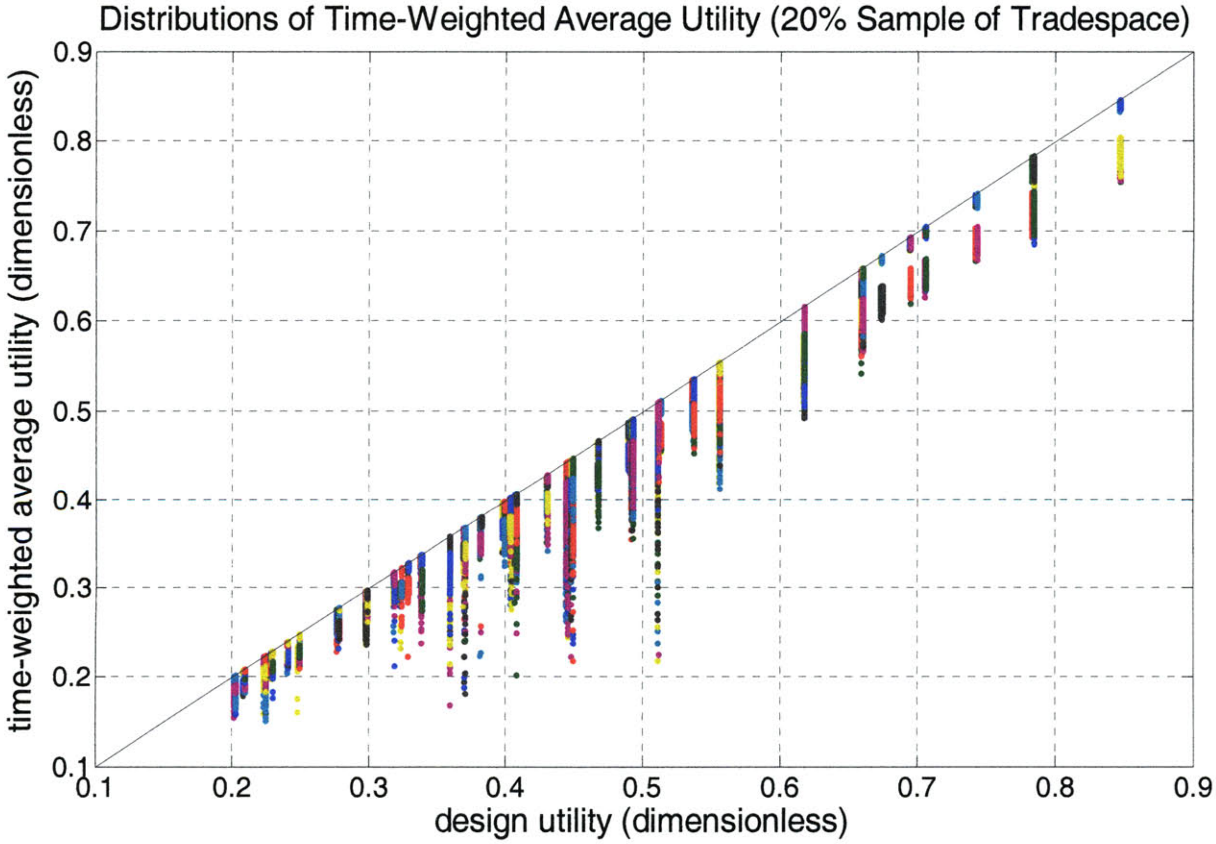


Figure 7-20. SR Distributions of Time-Weighted Average Utility

The results in Figure 7-20 are fairly uniform, showing a consistent pattern of highly-skewed distributions towards design utility. In contrast to the distributions of time-weighted average utility in the space tug computer experiment (Figure 5-14), the majority of utility losses are relatively small, as illustrated by the concentration of points near design utility. Interestingly, worst-case outcomes from the Monte Carlo simulation vary across the tradespace. While the tail-end of time-weighted average utility distributions for high design utility constellations (>0.6) fall only slightly below design utility values, the tail-end of distributions for mid-range design utility constellations (0.3-0.6) may extend down to 0.2 time-weighted average utility. This result underscores the ability of large, distributed constellations (in the high utility region) to sustain satellite losses with minimal impact on coverage statistics. Conversely, the impact of satellite losses on target acquisition time and target track life on intermediate-sized constellations in the mid-utility region is much greater. Utility losses in the low utility region are small. Although consisting primarily of small constellations, low-utility designs counter-intuitively have low sensitivity to satellite losses because of their baseline attribute performance levels. In particular, these designs deliver most of their value by their radar performance in the number of target boxes, minimum detectable target velocity, and minimum detectable radar cross section. Since these attributes are calculated at the satellite-level and performance in the constellation-level attributes is already low at beginning-of-life, constellation degradation has a less significant impact on time-weighted average utility.

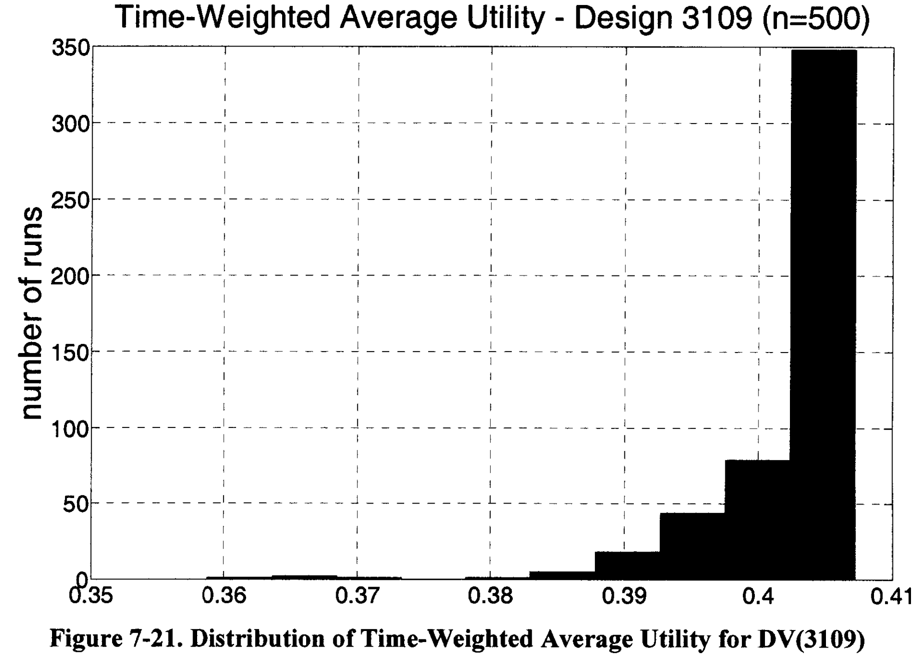


Figure 7-21. Distribution of Time-Weighted Average Utility for DV(3109)

Figure 7-21 shows the histogram of time-weighted average utility for DV(3109), a representative example of the skewed, long-tailed distributions across simulation runs. As shown in Table 7-13, DV(3109) consists of a large Walker constellation falling in the mid-utility range.

Table 7-13. Properties of DV(3109)

	Design Alternative #3109	
design variables	orbit altitude	1500 km
	Walker constellation	27/3/1
	transmit frequency	10 GHz
	antenna area	40 m2
	antenna type	AESA
	radar bandwidth	500 MHz
	peak transmit power	10 kW
	tugable	no
	comm. architecture	direct downlink
	tactical link	yes
	shield thickness	5 mm
	satellite spares	0
	lifecycle cost	$25.4B
	design utility	0.43

While the time-weighted average utility distributions are characterized by highly-skewed and long-tailed distributions, the distributions of threshold availability are much more limited in range. Given the size of the constellations and the setting of the emergency value threshold at zero utility, virtually all constellations are able to exceed the emergency value threshold following satellite losses from orbital debris. However, the emergency value threshold is violated for constellations relying exclusively on a direct downlink in the presence of global signal attenuation. Therefore, threshold availability values become an indicator of whether constellations utilize a relay backbone for communications.

Having examined the distributions of the survivability metrics, a percentile reporting level is established for each metric. Reflecting the risk aversion associated with failing to meet emergency value thresholds due to disturbances from the natural space environment, the reporting percentile for threshold availability is set at the 1st percentile (*i.e.*, 99% of the runs perform above the reported availability level). Given that utility losses within permissible thresholds are less severe, the reporting percentile for time-weighted average utility loss is set at the 95th percentile (*i.e.*, 95% of the runs experiences utility losses below the reported level). Sensitivity of the results to the percentile reporting level is performed during tradespace exploration by producing a survivability tear(drop) tradespace for multiple reporting percentiles and analyzing variance across the sets of Pareto-efficient designs.

7.2.8. Phase 8: Explore Tradespace

Having evaluated the cost, utility, time-weighted average utility loss, and threshold availability of each design alternative, integrated trades are made among the satellite radar constellations. Designs in the Pareto-efficient region are examined for prescriptive insights, and interesting designs are flagged as candidates for more detailed design. Following the survivability tear tradespace analysis, response surfaces are drawn to examine the impact of the survivability design variables on time-weighted average utility.

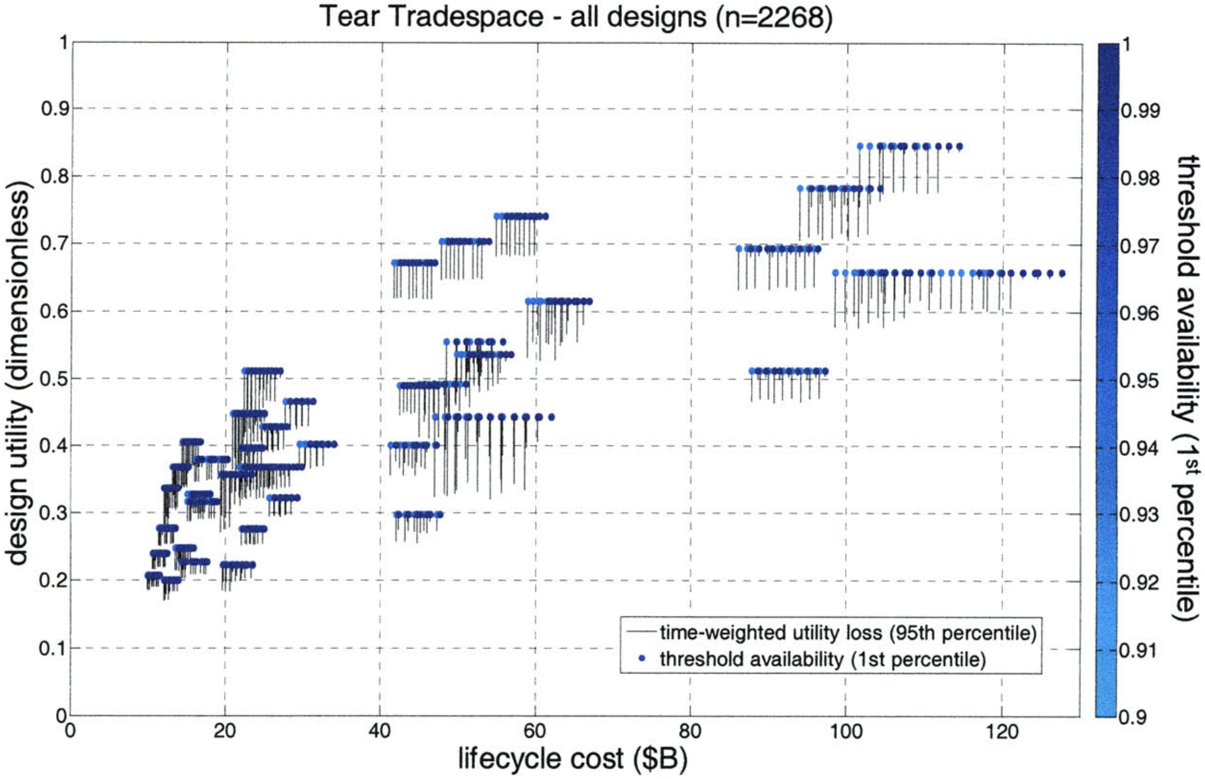


Figure 7-22. Survivability Tear Tradespace – Satellite Radar

Figure 7-22 presents the survivability tear tradespace for satellite radar. Addressing the need for trading lifecycle cost, performance, and survivability of design alternatives, deterministic cost and design utility data are integrated with the probabilistic metrics of time-weighted average utility loss and threshold availability. Preserving the cost and design utility axes of the baseline tradespace, the survivability metrics are incorporated using shade (threshold availability–1st percentile) and a line (for 95th percentile time-weighted average utility loss) drawn to time-weighted average utility.

A close inspection of Figure 7-22 yields several insights. Several clusters of similar design with fixed utility and variable cost are visible, reflecting insensitivity of utility to communications flexibility, bumper shielding, and constellation spares. While baseline utility remains fixed as the cost of these survivability enhancements are added to a given constellation, performance in time-weighted utility loss and threshold availability varies. As design options progress towards the interior region of the tradespace (*i.e.*, to the right, away from the Pareto front of cost and utility), survivability performance generally improves. The effect is not uniform, however, with several constellation clusters in the lower-end of the Pareto front unable to eliminate utility losses even with all survivability design variables at the highest setting. Most importantly, the tear tradespace shows that the time-weighted average utility of alternative satellite radar constellations (realized in operation) is different from the baseline utility achieved by the designs before disturbances are considered. Therefore, depending on the importance of survivability *vis-à-vis* cost and utility, the rank order preferences of the decision-maker on the static design space (*e.g.*, baseline tradespace in Figure 7-11) are subject to change.

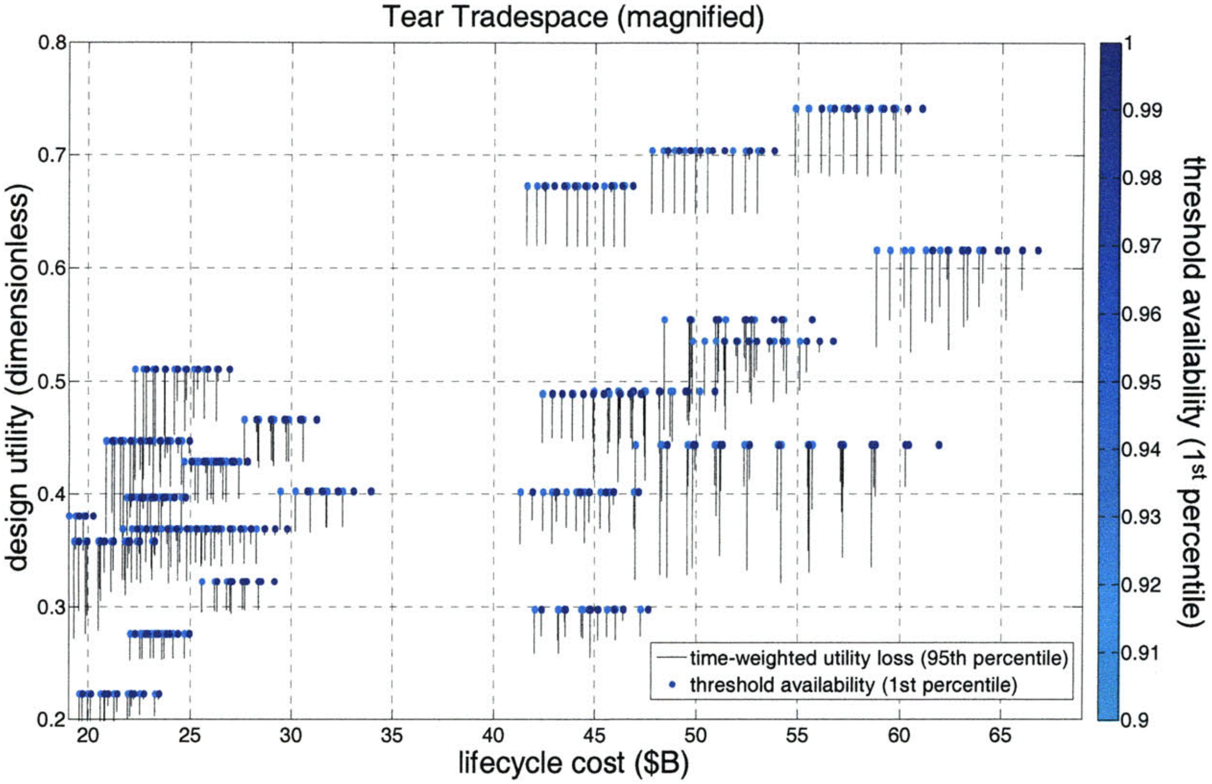


Figure 7-23. Magnified Survivability Tear Tradespace

Figure 7-23 magnified a portion of the Pareto front region of the tear tradespace. Accordingly, the high level trends observed in Figure 7-22 may be observed in more detail for a smaller portion of the tradespace. Each horizontal cluster of constellations grows in cost and improves in the survivability metrics as survivability variables are increased. In particular, lifecycle costs grow 15-30%, threshold availability increases from ~0.90-0.95 to ~1.00, and utility losses decreases a variable amount. Interestingly, many highly survivable systems are located in the middle of the horizontal clusters (rather than on the right side of highest cost).

To mitigate the complexity associated with visualizing the variation in cost, utility, and survivability performance—both within clusters and across the entire tradespace—filters may be applied to reduce the number of designs under consideration. For example, if designs located off the Pareto front of cost and design utility are eliminated from the tear tradespace, only 198 of the 2268 designs remain (see Figure 7-24). However, this filtering is undesirable given that the remaining designs are frequently the least survivable. If utility loss is applied as a third optimization axis to the filter, a three-dimensional region of Pareto efficiency consisting of 290 designs is identified (Figure 7-25). (This region includes a larger number of designs since it includes the original Pareto front of cost and utility as well as the new Pareto front of cost and utility, and "compromise" designs lying on the projected surface between the two planes.)

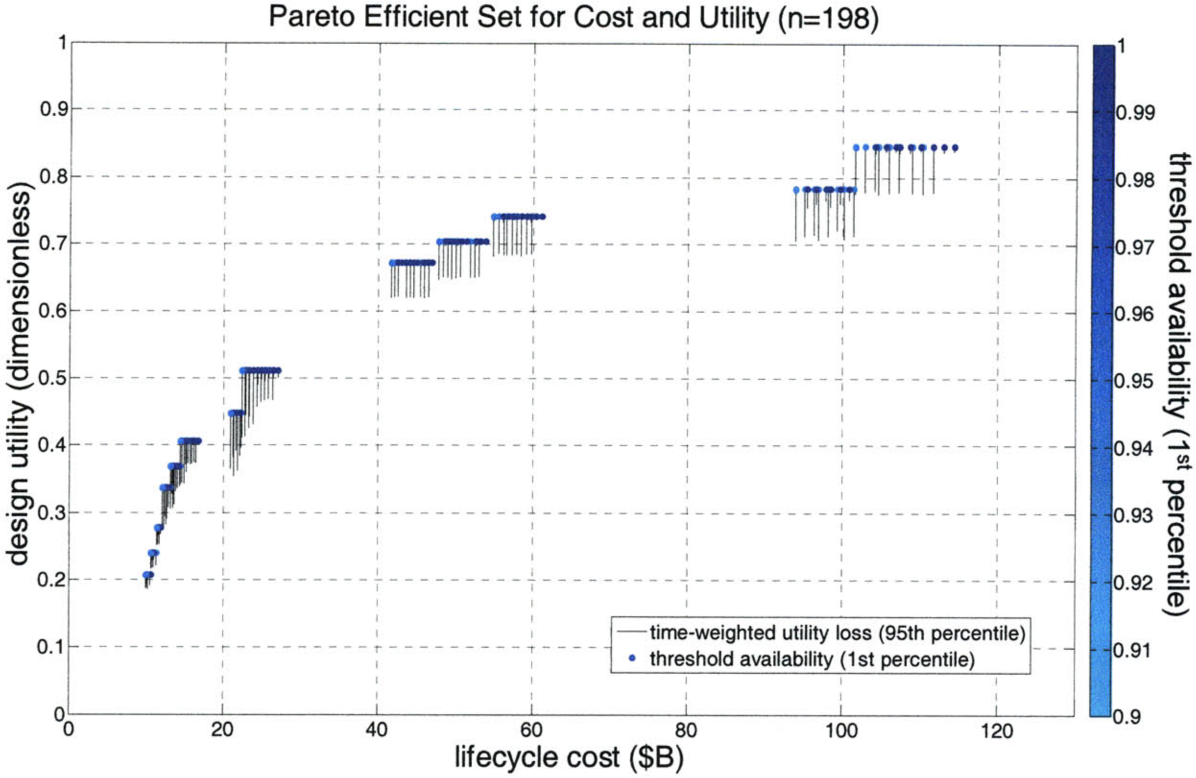


Figure 7-24. Pareto Front of Survivability Tear Tradespace

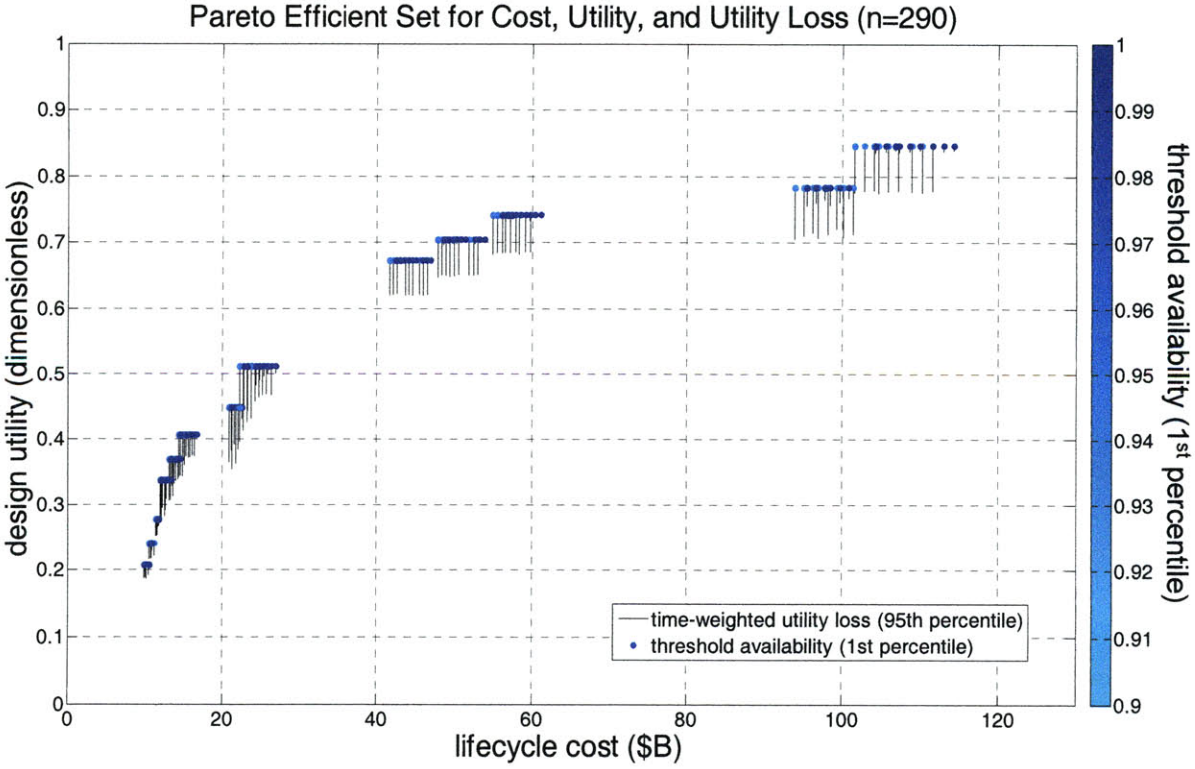


Figure 7-25. Three-Dimensional Pareto Surface of Survivability Tear Tradespace

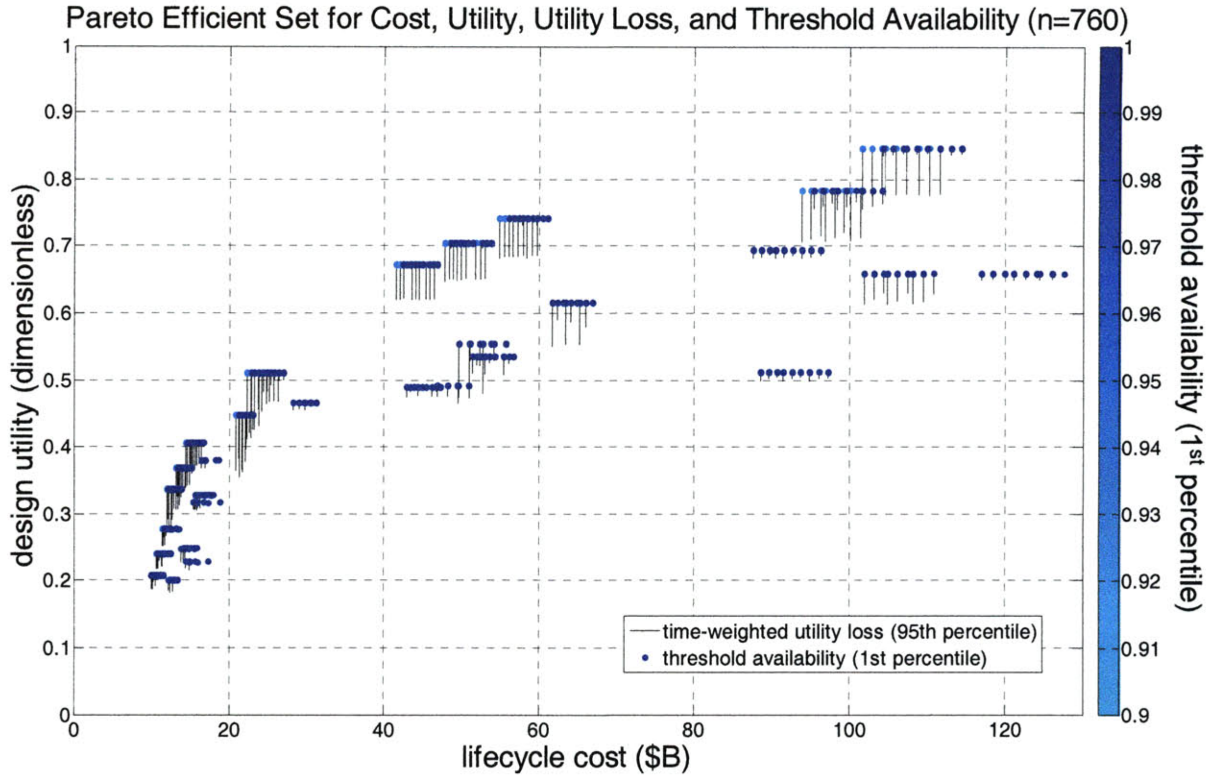


Figure 7-26. Four-Dimensional Pareto Surface of Survivability Tear Tradespace

Finally, if threshold availability is added as a fourth axis to the filtering criteria, 760 designs are identified in the Pareto region (Figure 7-26).

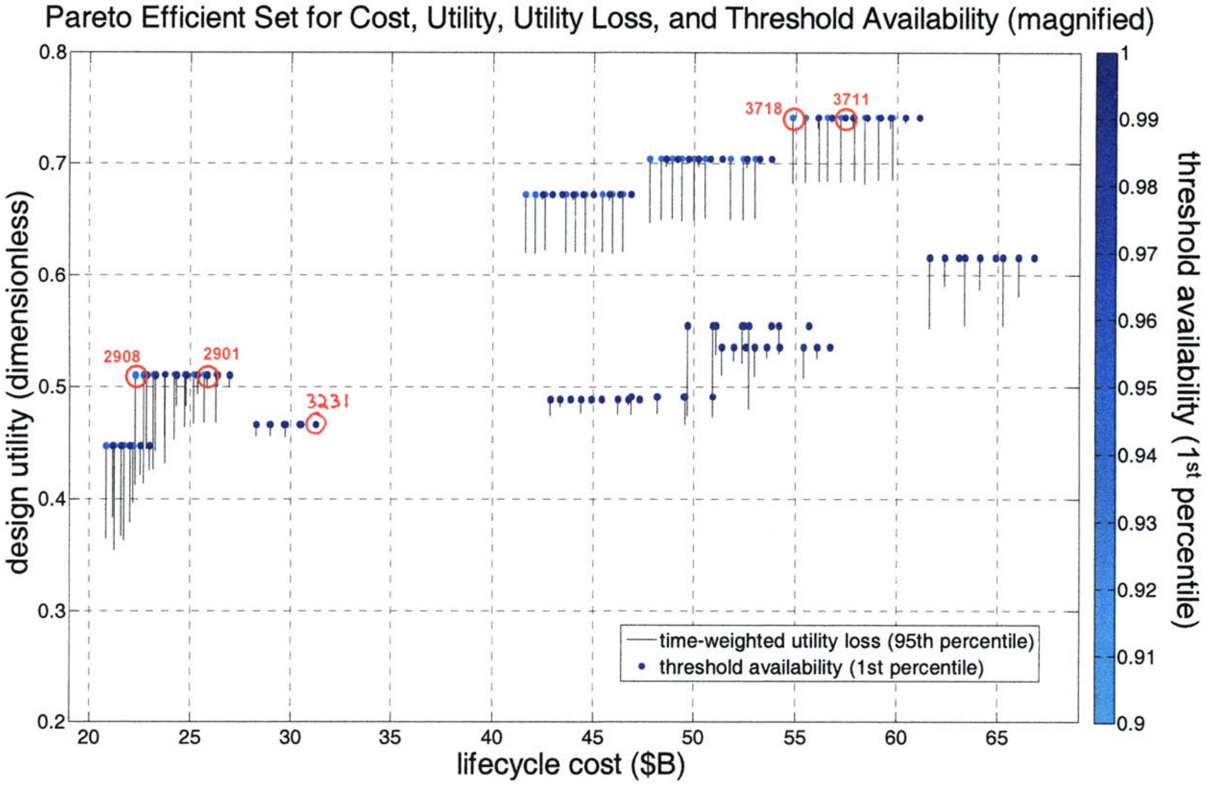


Figure 7-27. Magnified and Filtered Survivability Tear Tradespace

Having applied the filtering logic to identify a four-dimensional Pareto region of cost, utility, utility loss, and threshold availability, Figure 7-27 shows the designs that remain in the magnified region of the tear tradespace. While the filtering has greatly reduced the number of designs under consideration, dozens of "optimal" design remain within this central region of the tradespace. Five designs of particular interest are circled and labeled in Figure 7-27 for further investigation. Two of the designs, DV(2908) and DV(3718), are selected given their location in the traditional Pareto front. The other three designs are selected given their strong performance in the traditional metrics of cost and utility while also achieving high survivability. To complement the examination of DV(2908) and DV(3718), DV(2901) and DV(3711) are selected as survivable alternatives within the same constellation cluster. In addition, DV(3231) is selected as a survivable alternative located in the interior region. DV(3231) is included in the analysis because its high survivability is insensitive to the selected percentile reporting levels of the survivability metrics (see Figure 9-14 in Appendix F to see Figure 7-27 with time-weighted utility loss reported at the 99th percentile).

Table 7-14. Properties of Circled Design Vectors in Figure 7-27

Design Vector ID	2908	2901	3231	3718	3711
orbit altitude (km)	1500			1500	
Walker constellation	9/3/2	9/3/2	27/3/1	66/6/5	66/6/5
transmit frequency (GHz)	10			10	
antenna area (m^2)	100	100	40	40	
antenna type	AESA			AESA	
radar bandwidth (MHz)	2000			2000	
peak transmit power (kW)	20			20	
tugable	no			no	
comm. architecture	direct	relay	relay	direct	relay
tactical link	yes			yes	
shield thickness (mm)	1	1	10	1	
satellite spares	0	2	2	0	2
lifecycle cost ($B)	22.3	25.8	31.2	54.8	57.4
utility	0.51	0.51	0.47	0.74	0.74
utility loss (95th)	0.09	0.01	0.00	0.06	0.00
utility loss (99th)	0.12	0.02	0.00	0.07	0.01
threshold availability (1st)	0.95	1.00	1.00	0.95	1.00

Table 7-14 shows the design variable inputs and decision metric outputs of the satellite radar model for the five designs of interest. The designs are divided into two groups, with DV(2908), DV(2901), and DV(3231) located in the lower-left of the Pareto region, and DV(3718) and DV(3711) located in the upper-right region. Comparing columns allows explicit trades to be made between cost and survivability. For example, selecting DV(2901) in lieu of DV(2908) increases cost by $3.5B (through the addition of a relay communications system and the purchase of two satellite spares) but reduces utility loss to 0.01 and increases threshold availability to 1.00. Similarly, the additional $3.6B cost of DV(3711) reduces utility loss to effectively zero and increases threshold availability to 1.00.

Rather than improving the survivability of a Pareto front design exclusively through survivability enhancements, substituting DV(3231) for DV(2908) also improves survivability through the benefits afforded by a different system architecture. Although located close to the cost and utility values of DV(2908), DV(3231) has a different constellation structure consisting of more numerous, less-capable satellites. In particular, the Walker constellation is increased from 9/3/2 to 27/3/1, and the antenna area of each satellite is decreased from 100 to 40 m^2. The more distributed constellation structure combined with the investments in shielding and satellite spares yields a design that is highly survivable to even the most risk-averse decision-maker (Figure 9-14 in Appendix F).

While the primary goal of the tear tradespaces is to identify designs that achieve a good balance of cost, utility, and survivability, the preceding analysis also yielded prescriptive insights regarding the impact of the survivability design variables on a couple of point designs. Given that the fundamental goal of tradespace exploration is to gain a broad understanding of the design space, this analysis on two point designs is applied to the entire tradespace through the construction of survivability response surfaces.

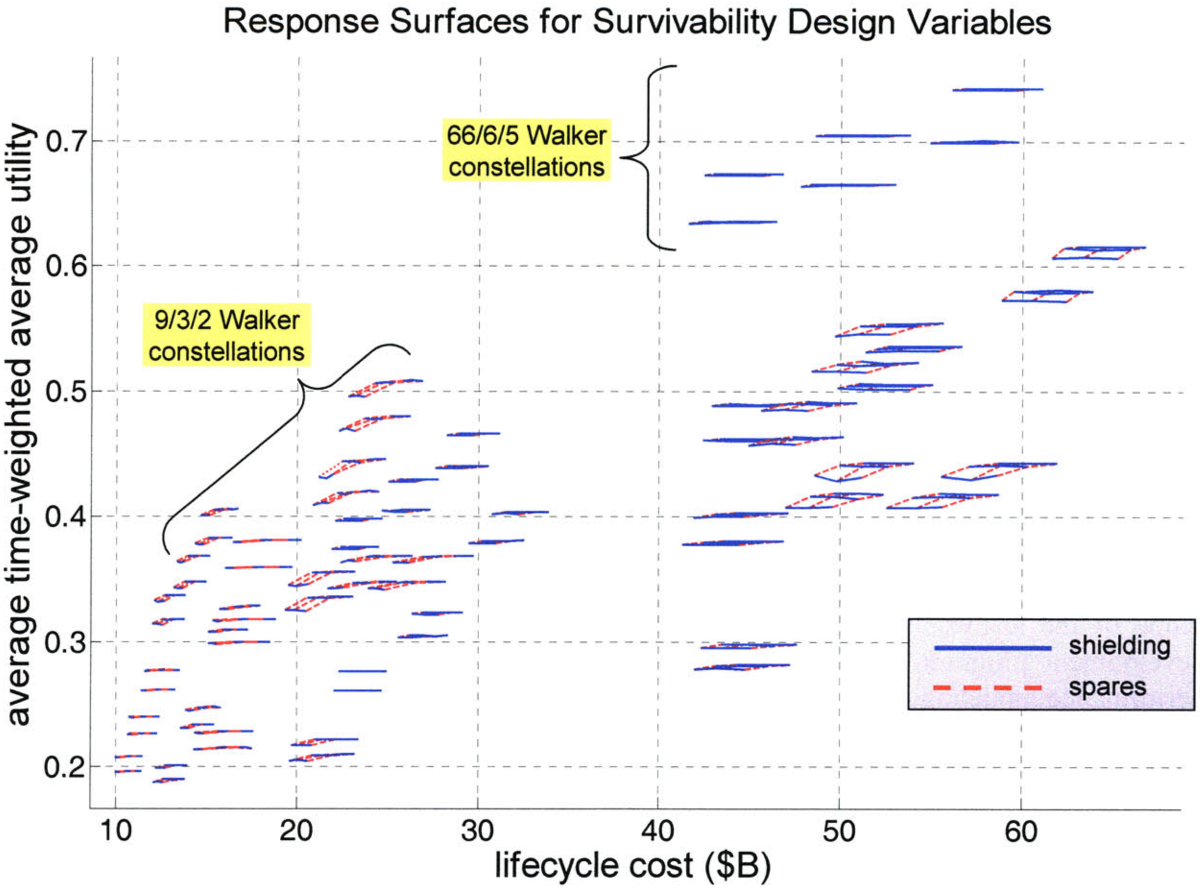


Figure 7-28. Survivability Response Surfaces for Satellite Radar

Figure 7-28 shows survivability response surfaces for each of the baseline designs. Each design point is located in terms of cost and average time-weighted average utility *(i.e.*, average value of time-weighted average utility over all Monte Carlo trials). Linked clusters indicate a common baseline design of constant Walker constellation type, altitude, antenna area, peak transmit power, and communications architecture. Each cluster consists of nine points, representing the full range of possible combinations of the two survivability design variables. The impact of survivability features may be observed by finding the lowest-cost point in each cluster to identify the baseline satellite radar design (which incorporates only 1 mm of shielding and no spares). Then, the response surfaces for shielding and spares may be viewed by examining the solid and dashed lines, respectively.

General prescriptive insights may be extracted from Figure 7-28 regarding the impact of shielding and sparing on the average utility achieved by design alternatives. Whether increasing to 5 mm or 10 mm, shielding universally adds cost but offers limited survivability benefits given the natural debris flux present in the orbits under consideration. The response surfaces for constellation spares are more interesting, revealing variable impact of the purchase of one or two additional satellites on average utility. For example, in the lower-left Pareto region of the tradespace featuring 9/3/2 Walker constellations, designs with spare satellites have higher average utility values. The impact is not linear, however, with diminishing returns associated with the purchase of the second spare. Different behavior is observed in the upper-right Pareto region consisting of 66/6/5 Walker constellations. While the same relative trend of increasing average utility with the purchase of spares may be observed under high magnification, the impact is extremely small. The response surfaces show similar behaviors in the interior region of the tradespace. With rare exceptions, shielding for natural debris adds cost with limited benefit to average utility while the impact of satellite spares varies as a function of constellation density.

7.3. Synthesis

Having applied MATE for Survivability to an analysis of military satellite radar, this section offers general insights for the system under investigation and for the methodology itself.

7.3.1. Satellite Radar Insights

Before providing specific insights on satellite radar, it is important to note two caveats. First, as discussed in Section 7.1, in addition to the survivability considerations that add complexity to the acquisition of any operational military system, attempts to acquire a military satellite radar capability over the past decade have been further characterized by fractured management, competing stakeholder needs, immature technology, and uncertain cost estimates. Therefore, the scope of the analysis in this chapter addresses only one part of what would be a complex development program. Second, as will be discussed in Section 8.2.2, cost estimation and performance modeling of future technologies are activities that can only be conducted at low to medium fidelity during conceptual design. The results, accordingly, reveal broad trends and provide general insights. While the results are valuable for a comparative analysis to guide the selection of a few promising alternatives for more detailed design, it would be unwise to associate absolute certainty with any of the projected cost, utility, and survivability values.

From the baseline performance modeling, the satellite radar case application revealed an extremely broad tradespace, with alternative designs varying in cost by an order-of-magnitude. Performance in the six GMTI attributes varied tremendously as a function of Walker constellation, power-aperture product of the radar sensor, and downlink options.

Given the results from the dynamic tradespace model, the satellite radar alternatives are survivable to the space environment (of orbital debris and signal attenuation). The survivability metrics applied to the utility trajectory outputs indicate that the enumerated constellations are able to meet the acceptability criteria for GMTI as specified in the utility functions. While time-weighted average utility is reduced following satellite losses in small and medium sized constellations, the reductions are small and the distributions of threshold availabilities remain above 90% at even the 1st percentile. However, when applied to sparse constellations, this finding is sensitive to changes in the decision-maker's acceptability ranges for target acquisition time and track life.

Although the satellite radar constellations are found to be survivable, the tear tradespace analysis shows that the rank-order preferences of the decision-maker on alternatives are subject to change when environmental disturbances are taken into account. By adding time-weighted average utility and threshold utility as additional decision metrics, designs in the interior region of the tradespace join the Pareto front designs in the "optimal" set. Resolution of these integrated cost, utility, and survivability trades requires dialogue with the decision-maker.

The tradespace model yielded several insights regarding the cost and survivability implications of the design variables. Counterintuitively, maximizing survivability design variable levels (and hence constellation cost) does not necessarily equate to the most survivable satellite radar system. In fact, shielding is found to have a very limited impact on time-weighted average utility. In contrast, supplementing direct downlink communications with a relay option is very important for mitigating signal attenuation. Investments in satellite spares have a variable impact, with sparse constellations benefitting the most from the option to rapidly reconstitute. There are diminishing returns, however, when purchasing additional spares.

Most interestingly, survivable designs that are most insensitive to decision-maker risk preferences (*e.g.*, percentile reporting level for time-weighted average utility) mitigate disturbances architecturally. The tear tradespace identified constellations that are co-located in the baseline tradespace (of cost and utility) with variable survivability performance. In particular, by sacrificing individual satellite performance and accepting moderate growth in lifecycle cost through selecting a more distributed constellation of less-capable satellites, it is possible to achieve higher levels of survivability.

7.3.2. Methodological Insights

Introduced in Chapter 6 as a formalization of the experimental tradespace analysis approaches pursued in Chapter 5, MATE for Survivability was successfully applied in this chapter to a satellite radar system. Building on a static MATE analysis, the methodology allowed survivability considerations to be incorporated into concept generation and tradespace evaluation. In concept generation, the designs principles revealed latent survivability trades in the initial design space and informed definition of a new design vector incorporating explicit survivability enhancements. In tradespace evaluation, the survivability metrics were applied to probabilistic utility trajectory outputs from a dynamic state model, enabling discrimination of thousands of design alternatives in terms of survivability.

In the case application, MATE for Survivability was applied following the conclusion of the baseline MATE analysis. An advantage of applying the methodology following an iteration of MATE is the ability to incorporate lessons learned into the formulation of the survivability analysis. For example, given the computational constraints associated with implementing a stochastic, path-dependent simulation of the health of alternative satellite constellations, it was very helpful to reduce the number of alternative satellite radar constellations (from tens of thousands to thousands) based upon insights gleaned from the initial tradespace exploration. However, a disadvantage of applying MATE for Survivability after completing a baseline MATE study is the challenge of adapting a static model to a dynamic analysis. Unless insensitive to the external environment, modeling the impact of disturbances changes the intermediate variables and attribute calculations. Given the need to assess system health over the entire lifecycle, a more efficient model with faster runtimes may be possible if survivability considerations are factored into the initial software development.

Many recommended practices for implementing MATE for Survivability emerged from the satellite radar case application. First, given that the survivability metrics are dependent on the percentile reporting levels, it is important to examine the sensitivity of the results to the selected percentile of the distribution (*e.g.*, stability of set of designs on four-dimensional Pareto surface when reporting time-weighted average utility loss at the 95th and 99th percentiles). Second, the broad insights that may be derived from the design variable impact tradespaces, tear tradespaces, and response surfaces, should be complimented by querying individual point designs. Close inspection of individual designs (including design variables, intermediate variables, calculated attributes, and performance metrics) allows the analyst to gain a deeper understanding of the causal relationships in the performance model as well as to verify model accuracy. Third, producing the filtered tear tradespace should not mark the end of the survivability analysis but rather mark a departure point for navigating the tradespace with the decision-maker. Although the 760 designs along the four-dimensional Pareto surface in the satellite radar tear tradespace are less than the 2268 in the unfiltered tradespace, they are significantly more than the 198 designs along the traditional Pareto front of cost and utility. Therefore, having identified the region of optimal trade-offs among cost, utility, and survivability, it is particularly important to engage with the decision-maker in the process of selecting a small number of alternatives for more detailed design.

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

8. Discussion

This chapter summarizes the unique contributions of the research (Section 8.1), discusses implementation issues associated with applying Multi-Attribute Tradespace Exploration for Survivability (Section 8.2), and proposes ideas for future work (Section 8.3).

8.1. Unique Contributions

There are four primary theoretical contributions of the thesis: (1) a clarification of the relationship between survivability and the other system properties known as the "-ilities", (2) a framework of survivability design principles for enhancing concept generation, (3) value-centric metrics for assessing survivability over entire system lifecycles, and (4) an integrated methodology to allow decision-makers to conduct trade-offs among system costs, benefits, and survivability.

8.1.1. Clarification of Relationship between Survivability and other "ilities"

As discussed in Section 1.1.4, recent research within the systems engineering and system analysis communities has sought to develop descriptive taxonomies and prescriptive methods for incorporating the "-ilities" into system design. Given the long development and operational lifecycles that characterize modern engineering systems, there is a need for systems that continue to deliver stakeholder value in the presence of change. Accordingly, beyond-first-use design criteria such as flexibility, robustness, survivability, and others are increasingly recognized as critical properties of successful engineering systems. However, while most decision-makers agree that the "-ilities" are important system properties, they are not well defined (nor easily evaluated) in isolation. Completed dissertations within ESD (Suh 2005; Wang 2005; McConnell 2007; Lin 2009) have generally focused on evaluation methodologies for a few important "-ilities" (*e.g.*, real options for scalability and flexibility). While Ross (2006) developed a changeability framework for defining and quantifying several "-ilities" (*i.e.*, robustness, flexibility, adaptability, modifiability, and scalability), addressing the particular challenges of survivability analysis was outside of the scope of these foundational efforts.

Definitions for survivability vary across the biological, network security, and aerospace and defense domains. As a result, a diverse range of domain-specific definitions exist for survivability (Table 3-1). Even within domains characterized by consistent definitions, a diverse array of survivability conceptualizations exist (*e.g.*, range of environments within which an entity remains operational; disturbance threshold above which an entity will cease to function; degree to which performance remains following a disturbance; time required to restore health following a compromising disturbance). To generalize existing definitions and operationalize survivability for value-centric tradespace exploration, survivability is defined generally in this thesis as the ability of a system to minimize the impact of finite-duration environmental disturbances on value delivery.

In the process of defining survivability for engineering systems (Chapter 3), several taxonomic distinctions between survivability and other "-ilities" are made. These distinctions are useful for placing survivability in the context of previous work as well as for the more general challenge of categorizing the "-ilities". For example, building on the seminal work of Simon (1996), the "-ilities Space" (Figure 3-1) allows "-ilities" to be classified in terms of changes in three dimensions: environmental context, stakeholder needs, and system design. Recent research has applied the "-ilities Space" to clarify and to structure the variety of "-ilities" in the literature in order to make the "-ilities" more useful to system analysts (McManus, Richards et al. 2007).

In this thesis, the "-ilities Space" is used to distinguish survivability from the closely related system property of robustness. Both survivability and robustness are measures of the ability of systems to reduce the sensitivity of their outputs to changes in the environment. However, although similar, survivability and robustness are distinct. While designing for robustness focuses on accommodating permanent changes in context (*e.g.*, continuous noise factors), design for survivability focuses on the mitigating finite changes in context (*e.g.*, impulse event). Therefore, survivability can be considered a special case of robustness with a finite condition on disturbance duration.

Precisely defining and distinguishing survivability from the other "-ilities" is an important step towards the rigorous specification of a larger class of "-ilities" in engineering design (*i.e.*, extending analyses beyond traditional "-ilities" such as reliability and maintainability). Furthermore, precisely understanding survivability is critical to enumerating a full set of survivability design principles.

8.1.2. Survivability Design Principles for Concept Generation

A prerequisite to the evaluation of the survivability of alternative concepts in tradespace exploration is the generation of survivable alternatives. As concept-neutral strategies of architectural choice, design principles augment the creativity of system designers by informing consideration of a broad tradespace of technically-diverse system concepts. These concepts, in turn, may be parameterized with design variables for subsequent tradespace exploration. While several conceptual frameworks of survivability design strategies exist (Ellison, Fisher et al. 1999; Ball 2003; Nakano and Suda 2007), these frameworks tend to exclude non-physical factors (*e.g.*, organizational resilience), to focus on domain-specific instantiations of survivability (*e.g.*, combat aircraft), and to offer no guidance on operationalizing each strategy for concept generation and evaluation in engineering design. Accordingly, there is an opportunity to extend, generalize, and operationalize existing frameworks of survivability design principles.

Chapter 4 presents a general, empirically-validated set of seventeen survivability design principles that either reduce susceptibility (*i.e.*, likelihood or magnitude of a disturbance occurring within a system boundary), reduce vulnerability (*i.e.*, sensitivity of system value delivery to disturbance-induced losses), or enhance resilience (*i.e.*, ability of a system to recover from disturbance-induced value losses within a permitted recovery time) (Table 4-7). Each principle is precisely defined *vis-à-vis* the temporal dimension of disturbance, allowing designers to consider survivability strategies that mitigate value-losses across the entire lifecycle of a hostile encounter (Figure 4-5). In addition, the seventeen principles are decomposed into structural and behavioral categorizes to inform two general survivability strategies: (1) *passive survivability* – closed (static) systems that resist disturbance based on projections of the operational environment, and (2) *active survivability* – open (dynamic) systems that cope with future uncertainty by stressing architectural agility (Table 4-8).

Having extended and generalized existing frameworks, the survivability design principles are operationalized in MATE for Survivability by generating survivable concepts from the design principles and then parameterizing these concepts with design variables (Section 6.4). The prescriptive value of the design principles is demonstrated in the satellite radar case application where 24 unique survivable concepts are generated from the principles and subsequently parameterized with 23 design variables (Section 7.2.4). 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.

8.1.3. Value-Centric Survivability Metrics for System Evaluation

Survivability is traditionally incorporated in engineering design as a binary metric using probabilistic risk assessment (Section 2.1.3). When examined in the context of dynamic, value-based tradespace exploration, this current approach for evaluating survivability is problematic in three critical areas. First, a binary characterization of system state fails to distinguish between systems that degrade gracefully (characterized by a reduced rate and/or magnitude of value losses) and fragile systems (where small disturbances may cause total system failure). The ability to make such distinctions is particularly desirable when navigating tradespaces of thousands of design alternatives. Second, although systems and their environments are constantly evolving, PRA tends to treat systems and environments as static and unchanging. Evaluating survivability as a fixed probability against a limited set of operational scenarios is inconsistent with the lifecycle perspective provided by dynamic tradespace exploration. Third, PRA lacks a value-centric perspective given the focus on the integrity of system components. Taking the value-centric perspective, system designers are freed to consider multiple paths to achieve the same value delivery.

Given these limitations, two value-based metrics are proposed for the evaluation of survivability in dynamic tradespace studies (Section 3.3). Given the general definition of survivability (Section 3.2.2), the metrics operationalize survivability as the ability to minimize disturbance-induced value losses while meeting required levels of value delivery during nominal and perturbed environment states, respectively. Applying the construct of quality-adjusted life years from the medical community, *time-weighted average utility loss* is introduced as a summary statistic of lifecycle value degradation. To characterize the ability of systems to meet critical value thresholds, *threshold availability* is introduced as a modification to traditional formulations of availability by allowing for changing stakeholder expectations over the course of a disturbance encounter. As demonstrated in the second space tug computer experiment (Section 5.3), the metrics exhibit three desirable criteria for evaluating survivability: (1) *continuous* (rather than a discrete, binary characterization), to enable distinction between systems that gracefully degrade and those that fail immediately following a disturbance, (2) *dynamic*, to allow assessment (and enhancement) of survivability across the lifecycle of a disturbance, and (3) *value-based*, to allow comparisons across technically-diverse system concepts.

8.1.4. Methodology for Integrated Cost, Utility, and Survivability Trades

While the proposed survivability metrics address several problems arising from PRA-based assessments of survivability, they fail to address other limitations of existing survivability analysis methodologies (Section 2.3). First, survivability models typically abstract the complexities associated with path-dependencies in the calculation of survivability by assuming independence among disturbance events. Second, current methods fail to facilitate decision-maker trades among system lifecycle cost, mission utility, and survivability. Instead, survivability is typically treated as a constraint on design.[48] Third, the reductionist approach of typical methodologies is more amenable to bottom-up analysis of system reliability than a holistic examination of architectural survivability to threats external to the system boundary.

As an advanced system analysis methodology that integrates the proposed survivability metrics with Multi-Attribute Tradespace Exploration, MATE for Survivability (Chapter 6) addresses these three additional limitations. In both the space tug computer experiment (Section 5.3) and the satellite radar case application (Chapter 7), path-dependencies are incorporated into the vulnerability and resilience portions of the survivability model. In particular, the work of Ross (2006) on dynamic MATE is extended by relaxing the assumption of pre-enumerated system states with Epoch-Era analysis. Given that disturbance encounters may lead to system states that would never be conceived of in design, a Markov state model is used to generate utility trajectories that characterize system value delivery through disturbance encounters. Subsequent Monte Carlo analysis ensures the generation of representative utility trajectories.

Another key contribution of MATE for Survivability is the tear tradespace representation for allowing decision-makers to trade between the traditional (deterministic) performance metrics of lifecycle cost and design utility and the (probabilistic) survivability metrics of time-weighted average utility loss and threshold availability (*e.g.*, Figure 7-22). Preserving the cost and design utility axes of baseline MATE tradespaces, the proposed survivability metrics are integrated using shade to depict threshold availability and a line connecting design utility to time-weighted average utility (*i.e.*, the utility loss, or "teardrop"). In applying the survivability tear tradespace to analyses of alternative space tug vehicles and satellite radar constellations, the rank-order preferences of decision-maker are subject to change. In particular, many designs that are "optimal" in the traditional Pareto front of cost and utility are shown to perform poorly in terms of the survivability metrics. Filtering the survivability tear tradespace reveals a four-dimensional surface of Pareto designs, allowing decision-makers to select designs located in the interior of the tradespace that efficiently compromise among cost, utility, and survivability. Furthermore, tear tradespace analysis may be used to examine tradespace sensitivities to variable decision-maker risk preferences. For example, since attitudes towards low-probability, high-consequence events may not be preserved across stakeholders, each survivability metric may be reported at multiple percentile levels, and the composition of the Pareto sets in the resulting tear tradespaces checked for stability or variance.

Finally, the satellite radar case application demonstrates the applicability of MATE for Survivability to generating prescriptive insights at both the system and architectural levels. Rather than delaying survivability considerations until after selection of a baseline system concept (which ignores the survivability implications of alternative system architectures), the tear tradespaces and response surface plots allow the effects of satellite-level and constellation-level survivability strategies to be examined in concert (*e.g.*, heterogeneous satellite downlink

[48] Historically, treating survivability as a constraint was appropriate given the systems under analysis (*e.g.*, piloted combat aircraft). However, investigating trade-offs among survivability, cost, and performance is critical to exploring the tradespace for current, autonomous systems (*e.g.*, UAV's).

option and different levels of constellation distribution, respectively). As illustrated for satellite radar, incorporating survivability considerations into the definition of the system concept is especially critical if the additive survivability design variables have a small impact on survivability relative to the fundamental system architecture.

8.2. Implementation Issues

In this section, four implementation issues associated with MATE for Survivability are discussed: (1) value elicitation for low-probability, high-consequence events, (2) fidelity of cost estimation and performance models, (3) minimum resource requirements, and (4) scalability of analytic effort.

8.2.1. Value Elicitation for Low-Probability, High-Consequence Events

One of the implementation issues of applying MATE for Survivability is that decision-maker preferences may change as the system passes through nominal and perturbed environmental states. While the process of eliciting attributes and associated utility functions is already complicated by the need for decision-makers to think using value-based, concept-neutral metrics (Ross 2003) and issues of measurement stability (Spaulding 2003), MATE for Survivability adds further complexity to the process since, as in Epoch-Era analysis (Ross 2006), the definition and scale of the utility axis are subject to vary across epochs (*e.g.*, space tug). Furthermore, unless the definition of utility is constant across epochs (*e.g.*, satellite radar), the permitted recovery time also needs to be elicited from the decision-maker.

As discussed in Section 3.3.4, two approaches may be taken for completing the value elicitation in MATE for Survivability. Most generally, the applicable multi-attribute utility functions across all potential epochs may be elicited from the decision-maker. However, excessive time may be required with the decision-maker to collect such data without a process for bounding the large set of future environmental states. An alternative is to make the assumption that the attribute set remains fixed across nominal and perturbed epochs, with only the acceptability range subject to change (Figure 3-7). Regardless of which approach is followed, a common challenge is to elicit the "true" value proposition of the decision-maker during, and in the immediate aftermath, of finite-duration disturbances

In conducting the utility interview (*e.g.*, lottery equivalent probability method), it is important to provide the proper context for the decision-maker to answer lottery questions (de Neufville 1990). Typically, this context is provided through a carefully crafted scenario (Ross 2003). However, thinking in terms of probabilities is difficult, and may be particularly challenging for decision-makers attempting to provide their "true" value proposition during low-probability, high-consequence events. While the complexity associated with eliciting multiple utility functions was not present in the satellite radar case application (where the military value proposition for GMTI is constant across disturbances in the natural space environment), future applications of MATE for Survivability may be subject to changing value thresholds (*e.g.*, survivability of transportation infrastructure to catastrophic terrorism).

When validating the elicited emergency value threshold and permitted recovery time is not possible or practical, alternative approaches towards eliciting decision-maker preferences during low-probability, high-consequence events may be pursued. For example, prior to conducting utility interviews, decision-makers might be placed in a wargaming environment that simulates the experience of low-probability, high-consequence events.[49] Also, if low-probability, high-consequence events warrant the development of scripted contingency plans (*e.g.*, nuclear command and control), such plans might inform establishing minimum system requirements. Finally, in addition to simulation and contingency planning, historical low-probability, high-consequence events might be consulted to specify emergency value thresholds and permitted recovery times.

8.2.2. Model Fidelity

Determining the appropriate level of model fidelity requires balancing between competing desires for rapidly comparing design alternatives and for generating more accurate tradespace insights. While lower-fidelity models require less time and resources (*e.g.*, parametric relationships and look-up tables), they may provide less prescriptive value than higher-fidelity models involving multiple developers and more computation power (*e.g.*, physics-based simulation). Given that MATE for Survivability is a conceptual design methodology for generating broad tradespace insights (at the expense of a deeper understanding of a small number of "point" designs), it is important that model development in phases five and six does not overwhelm the other six phases of the methodology. Furthermore, given that model accuracy is often determined by the weakest assumption in a model (and that the assumptions made in conceptual design are often characterized by a tremendous amount of uncertainty), the analyst should carefully select an appropriate level of model fidelity.

Following the approach taken by Ross (2006), models for tradespace exploration in this thesis opt for a heterogeneous approach to fidelity selection. While low-fidelity models of causal relationships are applied to most design variables and intermediate variables, higher-fidelity models are selectively developed for analyzing key attribute relationships. For example, the selection of launch vehicles in the satellite radar case application is determined using a simple algorithm to minimize launch cost given a set of mass constraints. Since launch vehicle type does not impact attribute performance but only lifecycle cost, details associated with structural loading requirements and thermal interactions are abstracted. In contrast, the computation of key constellation performance parameters (*e.g.*, target acquisition time, target track life) are modeled at a higher level of fidelity by propagating orbits and computing coverage statistics. The heterogeneous approach focuses fidelity improvements on the areas with the most significant impact on the tradespace results.

8.2.3. Resource Constraints

Implementing a MATE for Survivability analysis (Chapter 6) requires access to a critical set of resources: (1) a decision-maker, (2) analytic expertise, (3) computing power, and (4) time. First, the availability of a decision-maker is a foundational aspect of any value-driven tradespace

[49] A wargame is "an abstraction of reality based upon a suite of models, data, rules and procedures used to represent movement, detection, firing, and other aspects of the mechanics of combat. They include human decision-making and conflict, and do not produce rigorous, quantifiable or duplicate results" (Bowley and Lovaszy 1999). The historical benefits of wargaming in the 20th century for preparing the U.S. military enterprise for the next conflict are well-documented (Haffa and Patton 1998). These benefits include informing the science and technology research portfolio, acquisition purchases (*e.g.*, importance of aircraft carriers in lead-up to WWII), national security strategy, operational concepts, tactics, and doctrine.

study. Before initiating modeling activities, it is essential to have elicited a set of attributes to guide the enumeration of design alternatives and subsequent performance evaluation. If access to a decision-maker is limited or delayed, a proxy decision-maker may be identified to approximate the preferences. However, without direct decision-maker input, the tradespace results may be invalid. Second, applying MATE for Survivability requires software development expertise (*e.g.*, Excel, MATLAB) and domain-specific expertise in the type of system under investigation and in the environment in which the system will operate. Third, tradespace exploration requires significant computing resources to accommodate the geometric growth of the tradespace as design variables are added to the model. Computational efficiency is a particular concern for MATE for Survivability given the large number of Monte Carlo trials required to generate representative distributions of lifecycle performance. Fourth, whether constructing a low-fidelity model in a week or a higher fidelity model over several months, adequate time should be allocated in system development schedules to accommodate multiple iterations of a MATE for Survivability analysis. The computer experiments and case applications benefited tremendously from a spiral development approach in which initial tradespace models evolved iteratively. Not only does the spiral development approach allow the selective improvement of model fidelity (Section 8.2.2), but it also informs the enumeration and sampling of design variables towards higher-value regions of the tradespace.

8.2.4. Scalability

The effort required to implement MATE for Survivability may be scaled depending on the availability of time, expertise, and computing resources. While Chapter 6 provides an overview of the 29 tasks comprising a MATE for Survivability analysis (and Appendix E provides a detailed description of each task), selected tasks may be skipped or compressed for a minimalist analysis. As illustrated in Table 8-1, there are three areas where the level of effort may be scaled back while still preserving the fundamental analytic structure: (1) elicitation of value thresholds in disturbance environments, (2) explicit mapping of survivability design variables to disturbances, and (3) detailed sensitivity analysis on a subset of the tradespace.

First, to simplify the value elicitation phase, the analyst might assume that the multi-attribute utility function governing decision-maker value in nominal environmental states is applicable to the time period during, and immediately after, a disturbance. If this assumption is made, Tasks 1.4 and 1.5 may be skipped as the required and emergency value thresholds are both set at the common limit of attribute acceptability (*i.e.*, corresponding to zero utility for each attribute level). A dialogue with the decision-maker is required to determine the appropriateness of this simplifying assumption. For example, military decision-makers may have constant expectations on mission utility, regardless of the presence of environmental disturbances. In contrast, this assumption may be less appropriate for civilian infrastructures where performance requirements may be temporarily reduced following low-probability, high-consequence events (*e.g.*, natural disasters).

Second, the tasks comprising the application of the survivability design principles in phase four (Tasks 4.1-4.5) may be merged into the concept generation activities of phase two. Rather than revisiting the design vector following the characterization of the disturbance environment in phase three, the analyst might establish the final design vector in phase two. In particular, the mission statement may be consulted to infer the types of disturbances within the operational environment and to inform the incorporation of survivability considerations into the design vector. Since the survivability design variables may score very poorly in the design value mapping matrix (in terms of impacting attribute value), the analyst must apply engineering judgment to determine which dedicated survivability design variables to keep (if any). Omitting phase four eliminates the formal process of parameterizing the survivability design principles. While this omission eliminates a significant amount of work, it also eliminates the structured approach to quickly generate and screen a large number of survivable concepts before proceeding to concept evaluation.[50]

Table 8-1. Minimalist Implementations of MATE and MATE for Survivability

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

[50] Conversely, the survivability design principles need not be applied within a MATE for Survivability analysis to aid in the generation of survivable concepts.

Third, the selection of designs for detailed sensitivity analysis (Task 8.2) might also be eliminated in a minimalist implementation of MATE for Survivability. Given that the tear tradespace representation evaluates each design alternative in terms of the key performance metrics of cost, utility, and survivability, drawing detailed response surface plots for the impact of the survivability design variables may be superfluous.

In addition to these three aspects which might be eliminated to reduce the scale of effort required to implement a MATE for Survivability study, the scale of effort may also be reduced by limiting the scope of the remaining tasks. For example, the scale of effort required for modeling and simulation activities (phases five and six) may be reduced by limiting the number of survivability design principles that are parameterized and incorporated into the final design vector. While generating concepts from each design principle provides a structured way to consider a broad portfolio of options for mitigating disturbances, the inclusion of design variables for all seventeen design principles is not practical from an analytic perspective (given the limited engineering hours available in front-end system analysis) or from a computer runtime perspective (given the geometric growth of the tradespace as design variables are added). While a tension between the scope of the design vector and the fidelity of the system performance model always exists, a scaled-down version of MATE for Survivability might fix the system performance model at mid-fidelity while further narrowing the scope of the design vector.

8.3. Future Work

The scope of this thesis is limited to the challenges discussed in the problem statement (Section 2.4). However, in addressing these challenges, several promising areas for future work have emerged. This section describes six propositions for future work: (1) validate design principles outside aerospace domain, (2) parameterize CONOPS in design vector, (3) incorporate path-dependent environmental states, (4) model adversary decision-making, (5) extend scope for system-of-systems engineering, and (6) perform additional case applications.

8.3.1. Validate Design Principles outside Aerospace Domain

In Chapter 4, the survivability design principles are empirically tested by tracing them to the survivability features of aerospace systems that have successfully operated in severe disturbance environments. This iterative process is valuable for establishing the validity of the design principle framework. However, the stratified sampling of operational systems with established survivability records is limited to the aerospace domain. While no assumptions are embedded in the design principle framework to preclude application to systems outside the aerospace domain, future work should test the general validity and applicability of the seventeen principles.

There are several domains that might be pursued to further the testing and application of the survivability design principles. In terms of testing the survivability design principles, perhaps the most fruitful cross-cutting insights may be derived from systems that possess similar operational requirements yet are built by different industries. For example, parallels have been drawn between the reconfiguration and repair of aerospace/military systems and Formula One Racing pit stops (Csere 2000). In both cases, operators are under intense time pressure[51] and

[51] Pit stops in Formula One motor racing typically include replacement of four tires and refueling in approximately seven seconds (Catchpole, de Leval et al. 2007).

must decompose tasks into distinct modules with clear lines of responsibility and interchangeable actors. Furthermore, both are life critical operations that are frequently carried out by multinational teams. Future work might examine pit stop approaches towards situational awareness (*e.g.*, failure-modes and effects analysis for predicting pit stop tasks and risks), design refinements (*e.g.*, quick-release electrical and fuel connection), and process discipline (*e.g.*, fanatical training and repetition) for general insights regarding Type III survivability (Cross and Cross 1998).

In terms of applying the survivability principles outside of the aerospace domain, the hardening of critical infrastructures from natural disasters and terrorist attacks offers several areas for future research. Of particular concern are vulnerabilities in networked infrastructures that increasingly characterize banking and finance, transportation, power production and distribution, information and communications, and water and food supply.[52]

8.3.2. Parameterize CONOPS in Design Vector

Future work might also seek to incorporate concept-of-operations considerations into MATE for Survivability. Currently, the design vector is defined as a combination of design variables, which are designer-controlled quantitative parameters that reflect an aspect of a concept. Although defined generally, design variables in MATE analyses have traditionally focused on physical properties of alternative systems while ignoring behavioral properties by assuming a fixed CONOPS. Given the tremendous impact of operational behavior on system survivability (*e.g.*, see discussion of Nuclear Command and Control System in Section 4.2.2), it may be valuable to formalize CONOPS design in MATE for Survivability. There are many avenues for pursuing this line of research.

First, the survivability design principles might be refined for generating alternative CONOPS for subsequent tradespace exploration. For example, the seventeen principles might be decomposed into structural and behavioral categories, with the behavioral design principles tested for rigor and completeness against historical cases. There are several historical examples of engineering systems that achieved better survivability (without structural modifications) through modifications to operational behavior (*e.g.*, B-17's in WWII, B-52's in Vietnam). Second, given a set of CONOPS principles, alternative operational strategies might be specified for parametric tradespace analysis through the inclusion of operational variables within the design vector. Third, the evaluation of system alternatives (defined in both structural and behavioral terms) might be improved by incorporating operational costs in the tradespace analysis. For example, just as the survivability metric of time-weighted average utility loss serves as a statistic for the probabilistic distribution of multi-attribute utility, a metric for operational cost might serve as a statistic for the probabilistic distribution of system lifecycle cost. This is an improvement to the implementations of MATE for Survivability in this thesis which abstract uncertainties in operational cost by incorporating them into the (deterministic) lifecycle cost estimate.

[52] In addition to the technical challenges associated with evolving legacy infrastructures to more survivable states while meeting critical ongoing availability requirements, a critical public policy challenge remains: who will pay for hardening? One option is to mandate private investment through regulations promulgated by Congress. Another option is to provide government subsidies to share the burden. The current approach leaves the assignment of risk and blame to the insurance market and tort courtrooms.

In summary, just as MATE parameterizes the design space to gain a broad understanding of the physical design options available, it might also be possible to parameterize CONOPS for exploration of robust operational decision-making. Given the growing importance of improving the survivability of systems and of rapidly responding to threat (yet slow time-scales and expenses associated with modifying physical system architectures), a formal process for specifying and evaluating alternative operational behaviors would be a valuable addition to MATE for Survivability.

8.3.3. Incorporate Path-Dependent Environmental States

Another promising area of future work is to incorporate path dependencies in environmental states. Current implementations of MATE for Survivability feature a Markov state model of system health to model path-dependent vulnerability. A valuable extension would be to also address path-dependencies in system susceptibility. The approach taken for incorporating path-dependent susceptibility would likely vary depending on whether disturbances originate from the natural environment (discussed in this section) or from hostile adversaries (discussed in Section 8.3.4).

In the case of modeling the occurrence of disturbances from the natural environment, the Markov state model of system vulnerability might also be applied to system susceptibility. For example, in modeling satellite susceptibility to orbital debris, the occurrence of debris events is assumed to follow a (memory-less) Poisson process. However, susceptibility to debris may increase in the time period immediately following a breakup due to elevated local flux. Therefore, just as path-dependent vulnerability is modeled using a Markov state characterization of system health, path-dependent susceptibility might be modeled by specifying a finite number of environmental states with empirically-derived transition probabilities. Figure 8-1 provides a notional diagram for implementing this approach for orbital debris.

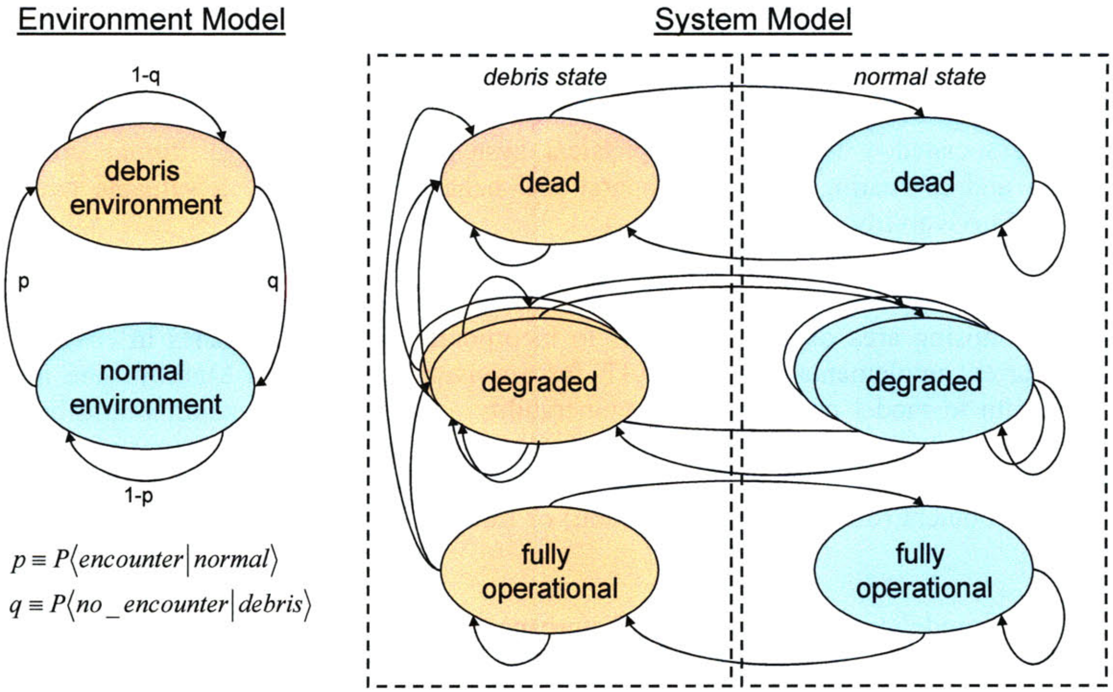


Figure 8-1. Incorporating Path Dependencies in Environment and System States

Instead of pursuing a discrete state modeling approach, path-dependent susceptibilities might also be incorporated into survivability analysis using system dynamics. System dynamics models are composed of a combination of positive (reinforcing) and negative (balancing) feedback loops in addition to state and rate variables (Sterman 2000). At its lowest level, a system dynamics model is a mathematical system of coupled, first-order, non-linear, ordinary differential equations presented in a graphical form accessible to policymakers.

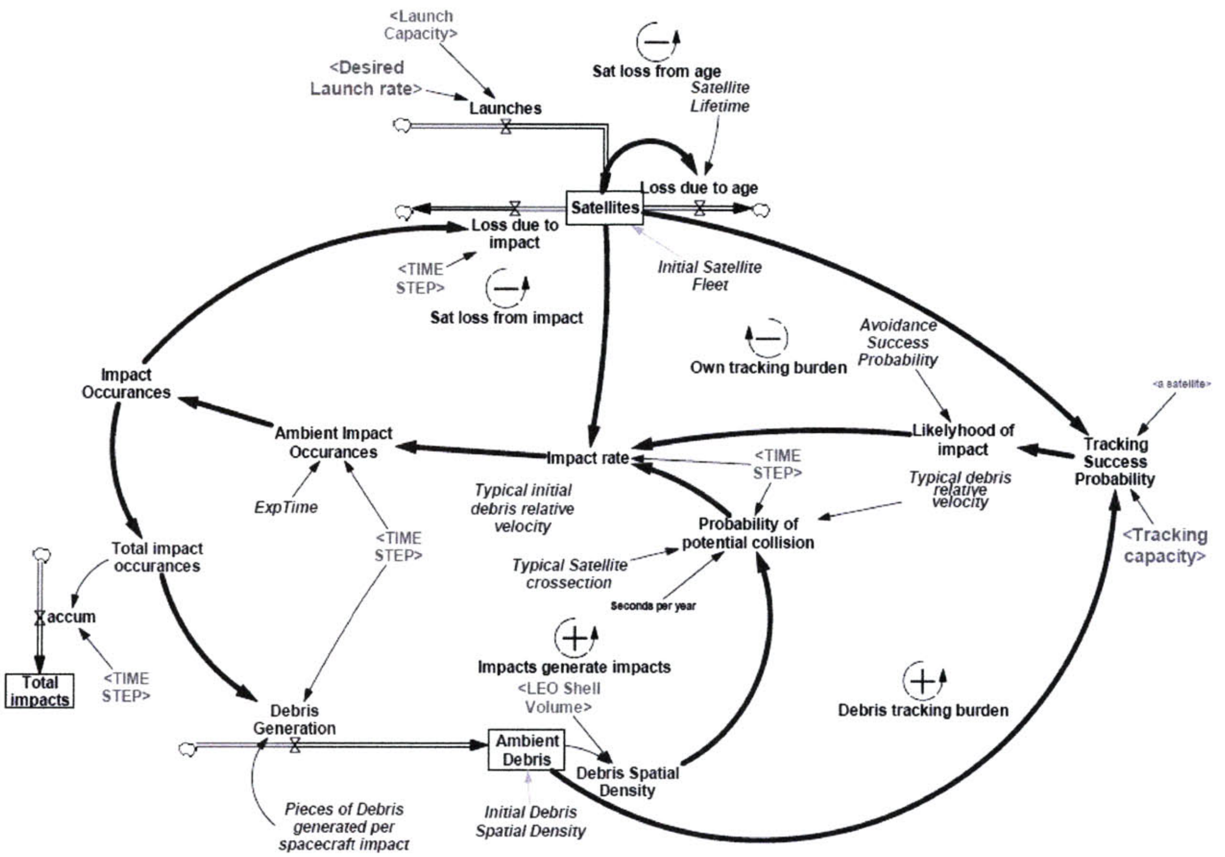


Figure 8-2. Path-Dependent Susceptibility Model of LEO Debris Environment

Figure 8-2 presents a systems dynamics model of satellite susceptibility to orbital debris.[53] Rather than modeling susceptibility as only a function of debris flux and exposed cross-sectional area, the probability of hit also varies over time as a function of previous impacts and the fidelity of a space-situational awareness (SSA) infrastructure. In particular, SSA is used to detect conjunction events and then warn threatened spacecraft, enabling operators to perform collision avoidance maneuvers. Given that SSA is a resource that provides a benefit that may be shared by several users, there is also the potential for its cost to be amortized over multiple users in a collaborative systems-of-systems (SoS). (The general challenge of incorporating survivability considerations into SoS engineering is discussed in Section 8.3.5.)

8.3.4. Model Adversary Decision-Making

If disturbances originate from intelligent adversaries in the environment, a different approach may be required for modeling system susceptibility. Since disturbances are the result of

[53] Figure 8-2 has four major loops: *Debris Tracking Burden, Own Tracking Burden, Satellites Lost from Impact*, and *Impacts Generating Impacts*. The first and last are reinforcing loops, while the middle two are balancing loops. *Impacts Generating Impacts* models the increased number of collisions given increases in the debris population. Debris generation leads to more debris generation—hence the loop is a reinforcing loop. As another reinforcing loop, *Debris Tracking Burden* also presents a problem. As debris levels increase with a fixed tracking capacity, the probability of successfully tracking a given piece of debris declines. Decreased tracking success leads to even more debris, which will further decrease tracking success.

calculated actions, it may be necessary to incorporate adversary decision-making into the susceptibility model. Five generic steps are suggested: (1) define threat types, (2) define strategies available to adversary, (3) define game structure, (4) determine how strategies are selected, and (5) update belief structure following hostile engagement.

In the first step of modeling adversary decision-making, different portfolios of systems that the adversary might deploy are defined (*e.g.*, Interceptors A and B, or Interceptors A and C). In the second step, the strategies available to the adversary for operating each portfolio of systems are defined (*e.g.*, shoot-look-shoot). Given the capabilities of the defender as perceived by the attacker, success probabilities for each attack strategy are assigned. In the third step, the strategic interaction between the attacker and the defender is modeled as a non-cooperative game. In particular, a static Bayesian structure is assumed in which agent behavior is characterized in terms of payoffs, actions, and beliefs. In the fourth step, a Bayesian-Nash equilibrium structure governs how strategies are selected, with agents maximizing their respective utility based on their beliefs. In the fifth step, Bayes Rule is applied (for an iterative game) to update beliefs following each hostile engagement. This generic approach for modeling adversary decision-making may also be applied to the defender. Given the discussion in Section 8.3.2, such an application may provide prescriptive insights for improving survivability through improved operational strategy.

8.3.5. Extend Scope for Systems-of-Systems Engineering

Just as information superiority offers a tremendous asymmetric benefit in terms of enhancing the effectiveness of modern military operations (Ballhaus 2005; Ryan 2006), it also represents a strategic vulnerability. Furthermore, this asymmetric advantage/vulnerability has not gone unrecognized by potential future adversaries. For example, Carter and Perry (2001) describe three asymmetric threats facing the United States: catastrophic terrorism, weapons of mass destruction, and "vulnerabilities in the complex but fragile information technology-based systems-of-systems." While the former two concerns have received a tremendous amount of attention from U.S. national security policymakers over the past decade, relatively little attention has been paid to the latter threat.

A systems-of-systems (SoS) may be defined as a synergistic configuration of systems in which constituent systems are independently managed and operated (Maier 1998). SoS engineering may be defined, in turn, as "the process of planning, analyzing, organizing, and integrating the capabilities of a mix of existing and new systems," with an emphasis on "discovering, developing, and implementing standards that promote interoperability among systems developed via different sponsorship, management, and primary acquisition processes (AFSAB 2005). SoS engineering has been the subject of studies in industry (Maier 1998), government (Chen and Clothier 2003; AFSAB 2005; DoD 2007b), and academia (Eisner, Marciniak and McMillan 1991; Sage and Cuppan 2001; Crossley and DeLaurentis 2006). While integrating coalitions of systems has always been inherent to complex military operations, SoS engineering has emerged as a formal practice following the host of integration problems in the First Persian Gulf War.[54]

[54] A host of integration problems occurred during Desert Shield and Desert Storm as C4ISR systems were deployed for the first time in support of tactical operations for a large-scale conflict. Older platforms were used for missions for which they were not designed (*e.g.*, Defense Support Program satellites for Scud detection), new technologies were applied piecemeal, and interoperability problems hindered full exploitation of information technology (Spires

To improve military preparedness for asymmetric countermeasures that future adversaries might employ against networked information systems, it is important that survivability considerations are incorporated into SoS engineering. Furthermore, given the increasing reliance of all modern enterprises on collaborative systems, incorporating survivability considerations into SoS engineering presents a general challenge and opportunity for systems engineering (Fovino and Masera 2006; Morris et al. 2007; Singh and Dagli 2007).

To understand the unique challenges posed by incorporating survivability considerations into SoS engineering, it is helpful to distinguish SoS engineering from traditional systems engineering. Table 8-2 provides seven criteria for using SoS methods and contrasts each to the traditional systems engineering paradigm (Eisner, Marciniak and McMillan 1991). Eisner's seven criteria provide an initial definition of SoS engineering as a unique class of problems related to, but different from, systems engineering. SoS are systems that are composed of other systems, and have some additional properties. For example, Maier (1998) describes the constituent systems of an SoS as exhibiting operational and managerial independence.[55] Traditional systems engineering techniques are difficult to apply to SoS design where authority is distributed among constituent systems. In particular, there is a misalignment of the top-down methods of traditional systems engineering with the bottom-up authority structure of SoS. This misalignment leads to additional challenges for the system architect who must not only manage the development of the SoS as a whole but also ensure that the needs of the constituents are met.

2001). Some of these integration problems were solved during the six month build-up to war (*e.g.*, early warning satellites were used successfully for detection of tactical ballistic missiles) while others were not (*e.g.*, paper copies of air tasking orders had to be flown from the command center in Riyadh to the decks of aircraft carriers) (Zinn 2004).

[55] Operational independence means that, should the SoS constituents be removed from the SoS, they still exist and are able to function as they did prior to joining the SoS. Managerial independence means that, not only can the constituents function independently, they continue to do so even while part of the SoS.

Table 8-2. Eisner's Seven Distinguishing Characteristics of Systems-of-Systems (1991)

	System of Systems Engineering	Traditional Systems Engineering
1	There are several independently acquired systems, each under a nominal systems engineering process.	Subsystems are acquired under centralized control.
2	Overall management control over the autonomously managed systems is viewed as mandatory.	The program manager has almost complete autonomy.
3	The time phasing between systems is arbitrary and not contractually related.	Subsystem timing is planned and controlled.
4	The system couplings can be considered neither totally dependent nor independent but, rather, interdependent.	Subsystems are coupled and interoperating.
5	The individual systems tend to be uni-functional and the systems of systems multi-functional.	The system is rather uni-functional.
6	The optimization of each system does not guarantee the optimization of the overall system of systems.	Trade-offs are formally carried out in an attempt to achieve optimal performance.
7	The combined operation of the systems constitutes and represents the satisfaction of an overall coherent mission.	The system largely satisfies a single mission.

The fundamental challenge posed by SoS to survivability analysis is the emergent behavior that arises in collaborative operations. While individual systems may be survivable in isolation, unintended behaviors during SoS integration and operation could adversely affect mission survivability. Since MATE for Survivability was only developed for single-system architecture trade-off decisions, there is a need to also consider mission dependencies on multiple systems and the dependencies of constituent systems on joint missions (Ellison, Fisher et al. 1999).

Considering the implications of Eisner's seven distinguishing criteria of SoS (Table 8-2) for each phase of MATE for Survivability (Chapter 6) informs specific propositions for future work. In the first phase of MATE for Survivability, Elicit Value Proposition, the metrics characterizing system-level performance should be supplemented by attributes, utility functions, and critical value thresholds elicited by the SoS architect for each joint mission.

In the second phase, Generate Concepts, the traditional, simplifying assumption of "clean-sheet" design should be eliminated to reflect the temporal mismatch of the constituent system lifecycles. While the SoS architect may have authority to develop new systems for a joint mission, several of the constituents are likely to be legacy systems with limited potential for physical modification (*e.g.*, satellite communications infrastructure). However, the SoS architect may retain control over how the legacy systems are operated. Therefore, building on the discussion in Section 8.3.2, specification of the design vector for SoS will involve enumerating design variables (for new systems) and operational variables (for both new and legacy systems).

In the third phase, Characterize Disturbance Environment, threats to both constituent systems and sensitive communication links should be enumerated. Determining a representative set of disturbances may be complicated by the geographic spread of many SoS.

In the fourth phase, Apply Survivability Principles, the design vector should be revisited with a particular emphasis on applying the behavioral principles to the generation of survivable SoS configurations.

In the fifth phase, Model Baseline System Performance, the value of SoS alternatives should be determined based on performance in joint mission attributes. Building on the modeling of SoS constituents, a theater-level fitness function might be specified that accepts inputs from the system-level performance models (Soban and Mavris 2000).

In the sixth phase, Model Impact of Disturbances on Performance, SoS considerations should be incorporated into models of susceptibility, vulnerability, and resilience. In many cases, collaboration with other systems might decrease susceptibility to attack (*e.g.*, through a stronger collective deterrent). However, in certain cases, collaboration with other systems might also increase susceptibility (*e.g.*, by introducing new failure modes). The space tug computer experiment (Section 5.3) provides an example of the importance of internalizing SoS factors in modeling survivability performance. In that implementation of MATE for Survivability, recovery strategies are enabled by purchasing insurance (*e.g.*, servicing for repair) which neglects the possibility of a common-cause failure across a shared infrastructure (*e.g.*, loss of launch site, impulsive demand for servicing). The problem of neglecting this common-cause failure could be mitigated by taking a system-of-systems approach whereby the survivability choices of individual decision-makers (*e.g.*, system level survivability investments, contributions to hardening infrastructure) affect the availability of recovery assets.[56]

In the seventh phase, Apply Survivability Metrics, time-weighted average utility loss and threshold availability should be applied to the distributions of utility trajectories for each constituent system as well as the joint mission (or missions).

The eighth and final phase of MATE for Survivability, Explore Tradespace, would require the development of new tradespaces to allow the SoS architect to trade among the local value propositions of the constituent systems and the global value propositions of collaborative missions. Rather than focusing exclusively on the impact of alternative survivability design variables, response surface analyses should also explore the impact of alternative sources of architectural leverage (*e.g.*, standards and protocols, incentives and side-payments).

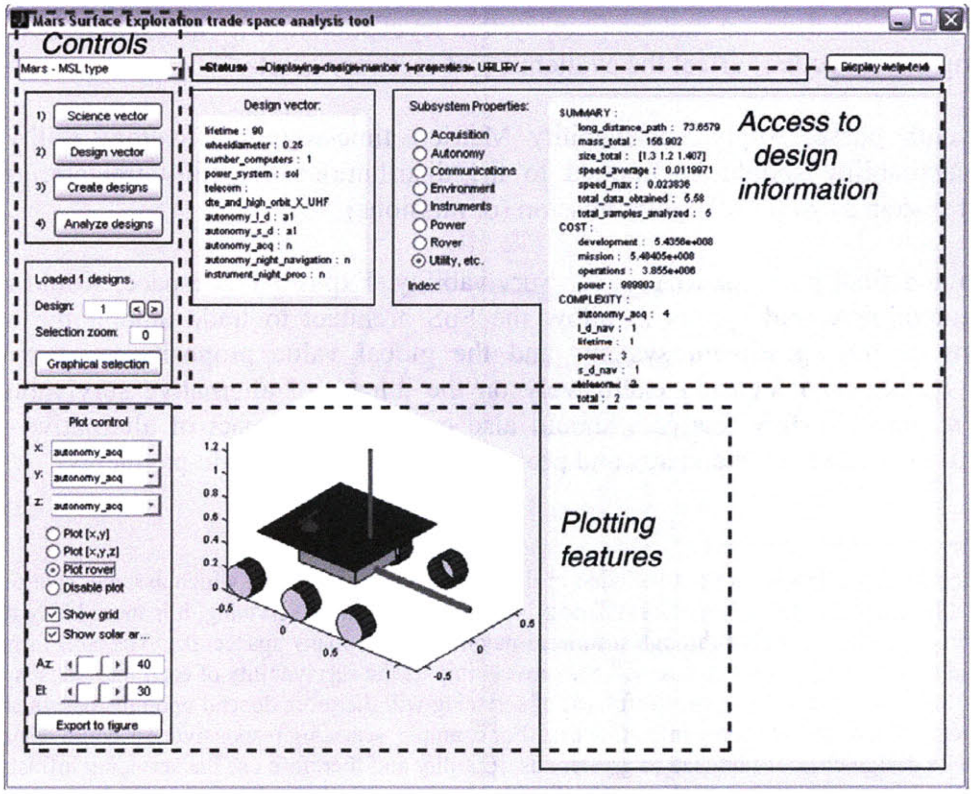
[56] Resilience path-dependencies are not included in the current space tug model which assumes that the servicer is always available when needed. Given the small cost-increment assigned to servicing, it is more likely that servicing will be a shared resource financed through insurance payments from many spacecraft. The SoS formed by these spacecraft and the servicing infrastructure will collectively impact the survivability of each individual spacecraft. In such a shared servicing architecture, the usefulness of servicing will therefore depend upon the design choices of the other customers utilizing the servicing infrastructure. For example, servicing responsiveness could decrease as other spacecraft make design choices that lead to greater susceptibility and therefore use the servicing infrastructure more often. Ensuring fair access to a jointly-financed infrastructure is a critical problem for designing survivable systems that depend on a shared resource to reduce vulnerability or enhance resilience.

8.3.6. Perform Additional Case Applications

There are many engineering systems that are strong candidates for conducting a MATE for Survivability analysis. From a research standpoint, several criteria might guide the selection of future cases:

- criticality of survivability considerations during conceptual design
- unit-of-analysis (with architecture-level preferred to fully leverage design principles)
- accessibility of decision-makers for value elicitation
- availability of models and data for prediction of technical performance
- availability of data on environmental disturbances
- amenability of system to dynamic state characterization
- phase in lifecycle development (with earlier preferred to impact design of real system)

Given these criteria, two potential future case applications are discussed: (1) Mars rovers and (2) operationally responsive space. Mars rovers offer a promising application area for MATE for Survivability given the host of severe environmental interactions characterizing roving operations. Over the past several years, NASA's Jet Propulsion Laboratory has developed parametric models to explore the tradespace of alternative Mars rover concepts (Figure 8-3). However, current analysis incorporate limited survivability considerations (*e.g.*, solar array degradation) (Lamamy 2007). Future work might apply MATE for Survivability to alternative rover concepts, including disturbance models of dust storms, extreme thermal cycling, and navigation obstacles.



Loaded 1 designs.

Design: 1

Selection zoom: 0

x: autonomy_acq

y: autonomy_acq

z: autonomy_acq

Az: 40

El: 30

```
Design vector:
lifetime : 90
wheeldiameter : 0.25
number_computers : 1
power_system : sol
telecom :
dte_and_high_orbit_X_UHF
autonomy_l_d : a1
autonomy_s_d : a1
autonomy_acq : n
autonomy_night_navigation : n
instrument_night_proc : n
```

```
SUMMARY :
    long_distance_path : 73.6579
    mass_total : 156.902
    size_total : [1.3 1.2 1.407]
    speed_average : 0.0119971
    speed_max : 0.023836
    total_data_obtained : 6.58
    total_samples_analyzed : 6
COST :
    development : 5.4356e+008
    mission : 5.48405e+008
    operations : 3.855e+006
    power : 989803
COMPLEXITY :
    autonomy_acq : 4
    l_d_nav : 1
    lifetime : 1
    power : 3
    s_d_nav : 1
    telecom : 2
    total : 2
```

Figure 8-3. Future Case Application: Mars Rovers (Lamamy 2007)

Operationally Responsive Space (ORS) offers a second promising case for applying MATE for Survivability. ORS has been defined broadly by the Department of Defense as "assured space power focused on timely satisfaction of Joint Force Commanders' needs... while also maintaining the ability to address other users' needs for improving the responsiveness of space capabilities to meet national security requirements" (DoD 2007a). The purpose of ORS is to reduce the time constants associated with space system acquisition, design, and operation to allow the national space architecture to keep pace with changing missions, environments, and technologies (GAO 2006). The fundamental idea is to trade off the reliability and performance achieved by satellites under the "Big Space" paradigm—the currently accepted way of conceptualizing, specifying, developing, and operating space systems—for the speed, responsiveness, and customization which may be achieved by architectures that incorporate elements such as small, modular spacecraft and low-cost, commercial launch vehicles (Figure 8-4). Given that the need to address space architecture fragility has been articulated by national leaders (Section 1.2), ORS offers an interesting case for examining how architectural agility might emphasized to address the mismatch between rapidly changing environments and the 15-25 year generational turnover of satellites (GAO 2006).

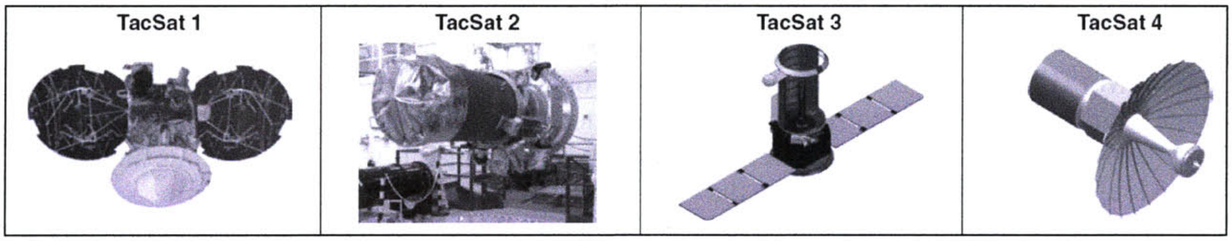


Figure 8-4. Future Case Application: Operationally Responsive Space (GAO 2006)

In addition to obtaining capability on-orbit quickly, ORS attributes include tactical control and assured access. Assured access refers to the potential ability of small, tactical spacecraft to be used to partially reconstitute Air Force space mission areas (*i.e.*, Intelligence, Surveillance, and Reconnaissance; Position, Navigation, and Timing; Communications; Environmental Sensing; Missile Warning; and Space Control) should adversaries negate existing space capabilities (Cebrowski and Raymond 2005). Implicit assumptions in the ORS and "Big Space" paradigms may be traced to their respective historical contexts and original beneficiaries. Table 8-3 provides a first-order approximation of the distinguishing characteristics of each approach.

Table 8-3. Distinguishing Operationally Responsive Space from "Big Space"

Characteristic	"Big Space"	ORS
Historical Context	Cold War	acquisitions crisis; fragilities inherent in integral, long-life designs
Original Beneficiary	White House	theater combatant commander
Programmatic Drivers	performance	cost, schedule
Innovation Dynamic	capability-pull	technology-push
Payloads	customized, satisfy multiple missions	Off-the-shelf; single-mission focus
Design Life	10+ years	1+ year(s)
Risk Tolerance (current)	risk averse	risk tolerant

Despite the purported benefits of ORS, progress on operationally responsive programs has been slow. In addition to a well-documented set of implementation hurdles (GAO 2006; Flagg, White and Ewart 2007), ORS progress is stymied by an uncertain value proposition to the U.S. military. Existing analyses in the literature conflict, with advocates finding that ORS "delivers the most utility to the warfighter per dollar spent" (Fram 2007), while a former deputy director for the Tactical Exploitation of National Capabilities at Air Force Space Command declares that "tactical satellites cannot serve the effect their proponents claim to want to achieve" (Tomme 2006). Mr. Gil Klinger, Director of Space Policy on the National Security Council from 2002 to 2005, states that operationally responsive architectures deserve, yet have not received, our "analytic due diligence."[57] This view is reinforced by an inability to find rigorous analyses of the value proposition for ORS across the Air Force space mission areas.[58] Furthermore, because one of the core values of ORS is an enhanced ability of the U.S. space architecture to sustain value delivery in hostile contexts—and given the limited ability of traditional survivability analysis methodologies to accommodate changing system configurations and operational environments—it is understandable that current evaluations of ORS are unsatisfactory.

[57] Personal conversation, 22 August 2007.

[58] The only study found, "The Case for Operationally Responsive Space: Cost and Utility" (Fram 2007), is severely limited in scope (*i.e.*, only examines one of six Air Force space mission areas), in design alternatives (*i.e.*, only three architectures considered), and in credibility (*i.e.*, assigns zero utility to peacetime intelligence collection—negating the value of strategic satellites except during war and skewing the results for a tactical solution). In addition, the availability of a reusable launch vehicle and low-cost commercial launch vehicles are assumed.

9. Conclusion

This chapter revisits the four research questions posed in Chapter 1 and draws general conclusions regarding survivability analysis. In answering each research question, key figures from previous chapters are displayed.

9.1. Revisiting Research Questions

1. What is a dynamic, operational, and value-centric definition of survivability for engineering systems?

The first research question aims to conceptualize and operationalize survivability for subsequent tradespace exploration. Survivability may be defined in physical terms as "the capability of a system to avoid or withstand hostile natural and manmade environments without suffering abortive impairment of its ability to accomplish its designated mission" (USAF 2005). Survivability may also be defined, more generally, as *the ability of a system to minimize the impact of finite-duration environmental disturbances on value delivery.* A value-centric definition of survivability is desirable during conceptual design because it provides a fundamental metric for relating system properties to desired stakeholder outcomes. Taking the value-centric perspective empowers decision-makers to compare technically dissimilar system concepts using a unifying set of attributes. The ability to consider multiple system concepts is particularly useful for survivability when original value delivery mechanisms may be blocked by a disturbance.

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

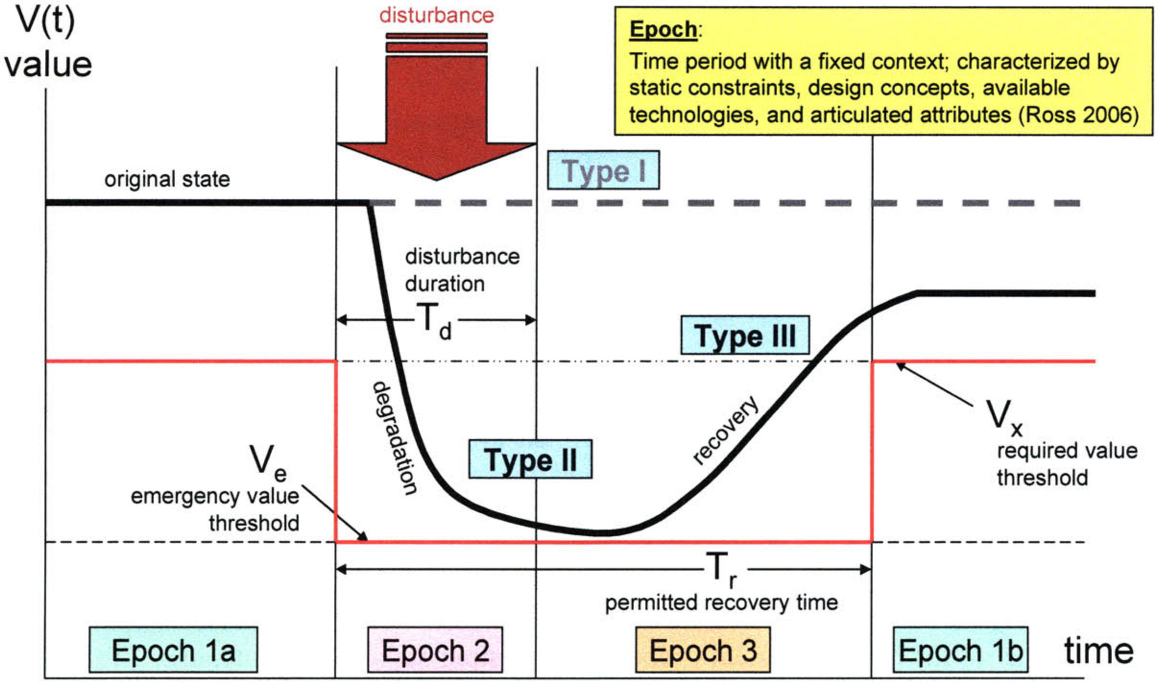


Figure 3-2. Conceptualization of Survivability

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

2. What design principles enable survivability?

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

Seventeen empirically-validated survivability design principles were identified in an iterative process of hypothesis generation and testing. Twelve design principles for enhancing survivability were initially deduced from a generic system-disturbance representation, from consulting the literature, and from retrospective case studies (*e.g.*, U.S. nuclear command and control system during the Cold War). Next, the validity of these initial results were tested by inductively mapping the survivability features of the A-10 Thunderbolt II combat aircraft and of the UH-60A Blackhawk helicopter to the design principle set. Results from this mapping identified missing design principles, taxonomic imprecision in design principle definitions, and deficiencies in the underlying system-disturbance framework—requiring an expansion to a set of seventeen design principles. Subsequent empirical testing validated the completeness of the seventeen design principles when applied to the Iridium satellite communications system and the F-16C Fighting Falcon. Table 4-7 shows the seventeen design principles, spanning Type I, Type II, and Type III survivability strategies.

Table 4-7. Validated Set of Survivability Design Principles

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

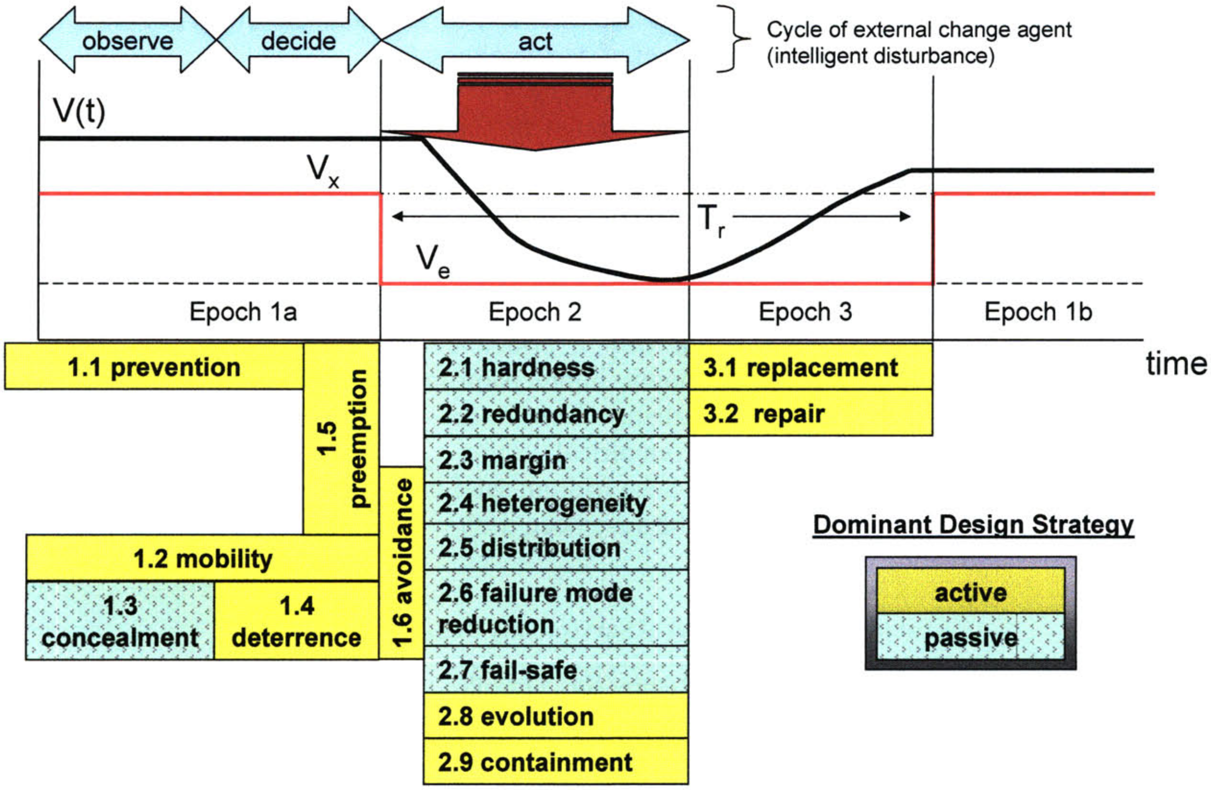


Figure 4-5. Mapping of Design Principles to Disturbance Lifecycle

Figure 4-5 depicts the time intervals during which each of the seventeen design principles may positively affect value delivery in a disturbance lifecycle. Each design principle is classified as either passive or active. A focus on passive principles will lead to the construction of closed (static) systems that resist disturbance based on projections of the operational environment. A focus on active principles will lead to the construction of open (dynamic) systems that cope with future uncertainty by stressing architectural agility to recover from disturbances. The distinction between passive and active survivability is useful because it specifies which design principles may be used based on the changeability of the architecture.

As demonstrated in the MATE for Survivability study of a satellite radar system (Chapter 7), 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.

3. How can survivability be quantified and used as a decision metric in exploring tradespaces during conceptual design of aerospace systems?

Survivability is evaluated based on the relationship between stochastic trajectories of system value delivery (*e.g.*, multi-attribute utility over time) and critical value thresholds elicited from a decision-maker (*i.e.*, required value threshold, emergency value threshold, and permitted recovery time). For example, Figure 5-12 shows a sample utility trajectory and set of critical value thresholds for an orbital transfer vehicle. The ten-year operational life is characterized by a series of non-catastrophic debris impacts and two restorative servicing operations.

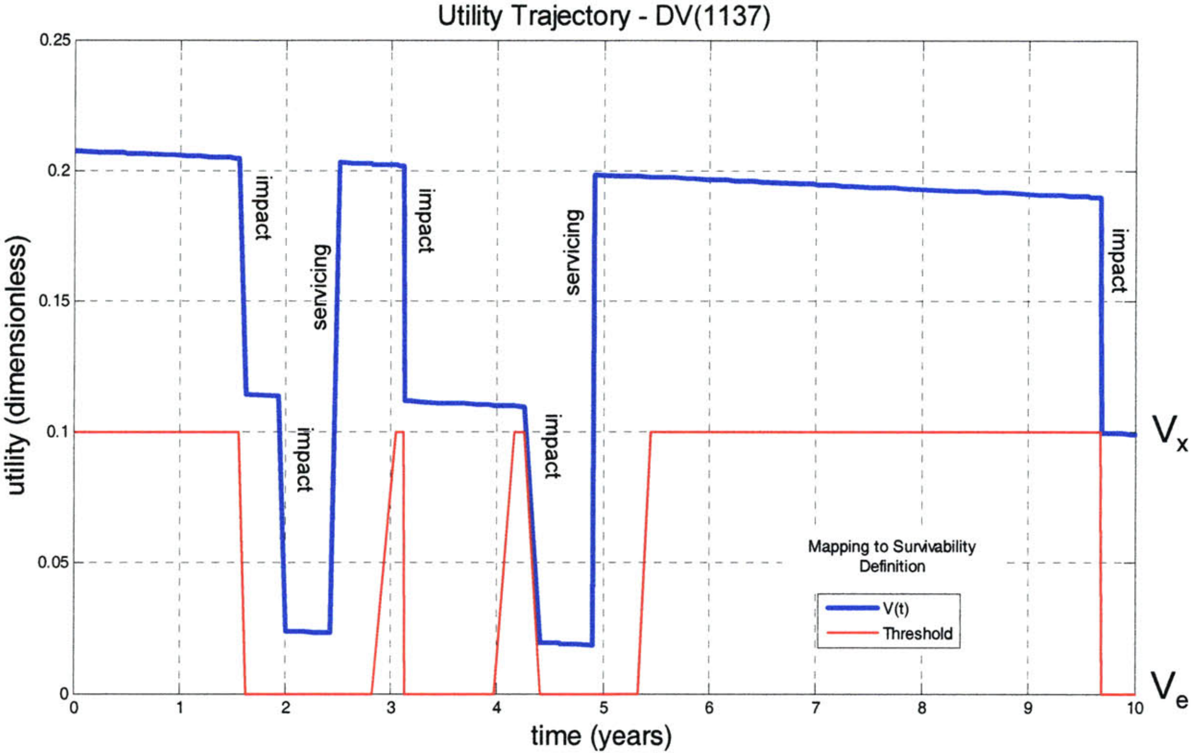


Figure 5-12. Sample Utility Trajectory

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

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

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

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

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

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

As survivability is a stochastic, path-dependent property, a single utility trajectory from a single design alternative is not necessarily representative or meaningful from a decision-making perspective. Rather, each utility trajectory constitutes one data sample from a continuous distribution of potential system lifecycles. Furthermore, there is a need to distinguish across collections of utility trajectories of different design alternatives in the tradespace. However, observing all of the utility trajectories generated in a MATE for Survivability study—typically 500 or more for each of several thousand design alternatives—is not practical. Therefore, time-weighted average utility loss and threshold availability are applied as aggregate measures for each set of utility trajectories. Figure 5-18 shows how the survivability metrics may be integrated with traditional performance metrics of cost and utility in a survivability "tear(drop)" tradespace.

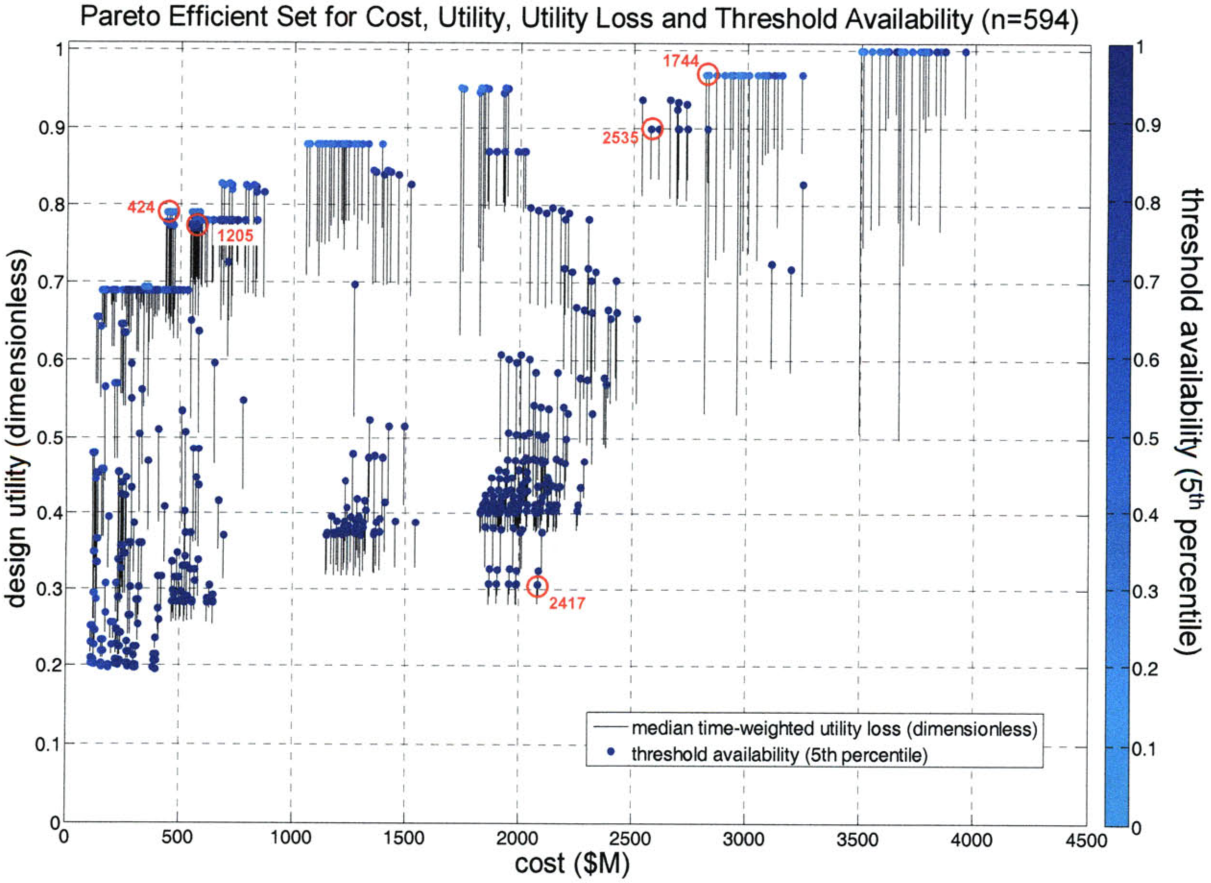


Figure 5-18. Four-Dimensional Pareto Surface of Survivability Tear Tradespace

The survivability tear tradespace provides a new approach for conducting survivability trades during conceptual design by integrating survivability considerations into the selection of the baseline system concept. (Use of the word "tear" is meant to describe regret associated with system utility loss.) The survivability tear tradespace preserves the axes in a traditional MATE analysis by plotting alternative system designs in terms of cost and utility. The new probabilistic survivability metrics are integrated using shade for threshold availability and a line drawn between utility and time-weighted average utility to indicate time-weighted utility loss. As illustrated in Figure 5-18, the large number of designs in the survivability tear tradespace may be filtered over the four-dimensional Pareto surface of cost, utility, time-weighted average utility loss, and threshold availability. This expanded region of Pareto efficiency reveals several interesting designs in the interior of the tradespace. While not located along the Pareto front of cost and utility, these designs join the "optimal" set based on performance in the survivability metrics.

4. For a given space mission, how can alternative system architectures in dynamic disturbance environments be evaluated in terms of survivability?

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

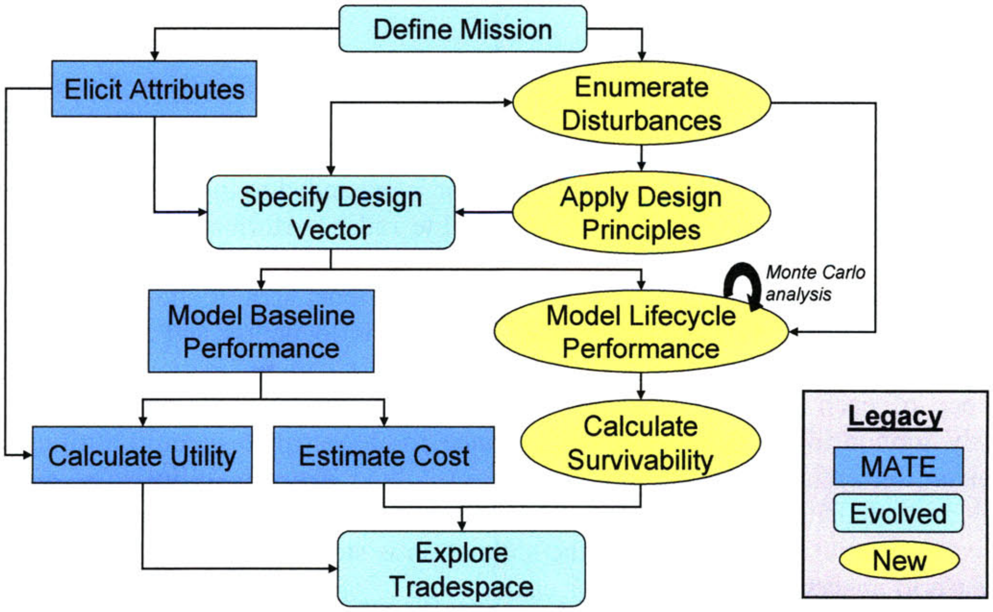


Figure 6-8. Multi-Attribute Tradespace Exploration (MATE) for Survivability

The satellite radar case application (Chapter 7) demonstrates the prescriptive insights that may be yielded from a MATE for Survivability analysis. Thousands of architectural alternatives are evaluated for a future military satellite radar capability, including various satellite designs, constellation structures, and supporting communications networks. Figure 7-17 provides a flow-chart representation of how survivability considerations are incorporated into the satellite radar tradespace by modeling lifecycle performance.

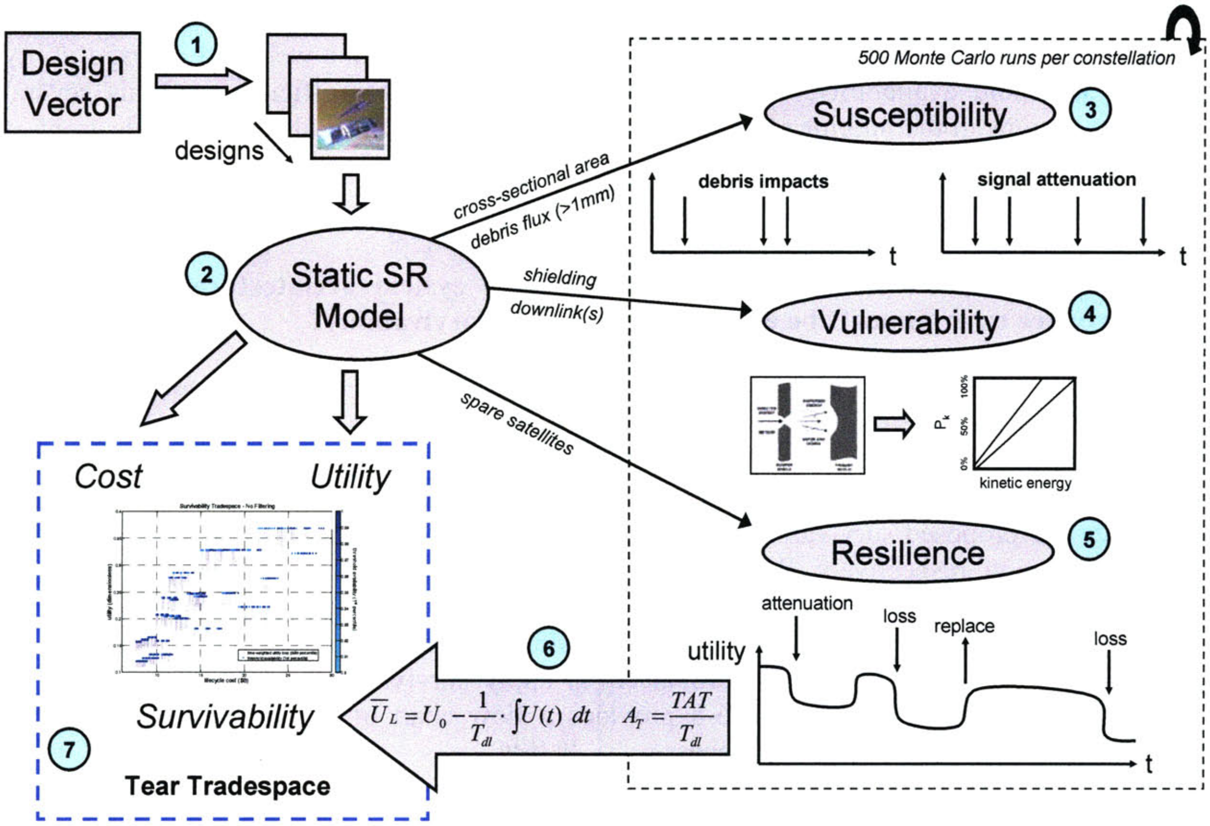


Figure 7-17. Incorporation of Survivability Considerations into Satellite Radar Tradespace

Treating the static tradespace model as a black-box, implementation of the survivability analysis involves seven general steps. First, the design vector is expanded to include survivability design variables. Second, a physics-based model of satellite radar performance is used to assess the total lifecycle cost and design utility of 3,888 design alternatives. Third, susceptibility to debris impacts is modeled as a function of the exposed cross-sectional area of alternative constellations and debris flux. Fourth, the vulnerability of the designs to debris and signal attenuation is calculated as a function of satellite shielding and available communications downlinks. Fifth, the resilience of each design is assessed based on the availability of satellite spares. By continuously monitoring constellation performance in the attributes, multi-attribute utility is assessed over the entire lifecycle. Sixth, time-weighted average utility loss and threshold availability are calculated at the end of each ten-year simulation as summary statistics for the utility trajectory output. As each run of the simulation is stochastic and path-dependent, a 500-run Monte Carlo analysis is performed for each design to obtain a representative distribution of utility trajectories. Seventh, the probabilistic survivability metrics are integrated with the deterministic metrics of lifecycle cost and design utility for integrated tradespace exploration.

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

9.2. General Conclusions

Counterintuitively, the risk-averse nature of the space industry exacerbates space architecture fragility by increasing the magnitude of potential downside losses.

The development of MATE for Survivability as general system analysis methodology is motivated within the space domain by the growing societal dependence on space-based services, the emergence of threats, and unintended consequences of the current paradigm. The risk-averse nature of the space industry has manifested in the common satellite design elements of subsystem redundancy, proven technology, and long design lives. As a result of these practices, the pace of generational turnover has slowed tremendously over the past half-century, increasing the magnitude of potential losses and reducing the speed at which capabilities might be reconstituted. Given the high cost of launch, traditional performance metrics of minimizing cost-per-function reinforce these trends by incentivizing the concentration of revenue-generating payloads onto fewer satellite platforms. While traditional approaches may optimize stakeholder value within fixed contexts, their value propositions are fragile in the presence of changing needs, markets, and environments.

The growing need for survivability in the space domain parallels the growing need for "-ilities" in engineering systems.

The misalignment of the rate of change of current space architectures and the rate of change in the environments in which they are deployed is shared by many terrestrial systems that are increasingly characterized by long design lives, dependencies with other systems, and large numbers of stakeholders. A common challenge for these engineering systems is the incorporation a broader set of "-ilities" (*e.g.*, flexibility, robustness) into the high-leverage phase of conceptual design. Just as survivability is a special case of robustness (with a finite condition on disturbance durations), the desire for robustness is, in turn, a subset of this general challenge of identifying the degree to which systems are able to maintain or even improve function in the presence of change. System analysis methodologies that can generate and evaluate various "-ilities" during conceptual design are a prerequisite to the deliberate selection, development, and deployment of dynamically relevant systems.

The evaluation of survivability requires assessing system value delivery across hostile contexts that may modify both system performance and stakeholder expectations.

Achieving survivability requires meeting minimum stakeholder expectations during nominal and disturbed environmental states. Assessing survivability involves a confluence of two dimensions: (1) the mapping of a system's form as mediated by the operational environment to determine technical performance, and (2) the mapping of stakeholder expectations as mediated by the operational environment to technical performance. While technical performance may be projected using physics-based models, stakeholder expectations such as emergency value thresholds and permitted recovery times are specified by the decision-maker. Accordingly, there are distinctively objective and distinctively subjective aspects to a value-centric calculation of survivability.

The survivability design principles enable generation of technically-diverse sets of system solution concepts that may be evaluated within a common tradespace using the value-based survivability metrics.

The value-centric perspective enables the unified evaluation of technically diverse system concepts through the application of decision theory to engineering design. Just as the survivability design principles operationalize the value-centric perspective for concept generation by enumerating concept-neutral strategies of architectural choice, the survivability metrics operationalize the value-centric perspective for concept evaluation by comparing thousands of design alternatives along the common axes of time-weighted average utility loss and threshold availability. Avoiding the limits of local "point" solutions that severely constrain the range of alternatives under consideration, these metrics may be universally applied to design alternatives incorporating various combinations of passive and active survivability features that span susceptibility reduction, vulnerability reduction, and resilience enhancement strategies.

Evaluating survivability during concept selection allows the identification of inherently survivable architectures that efficiently balance competing performance metrics of lifecycle cost, mission utility, and operational survivability.

Two recurring trends in applying MATE for Survivability underscore the importance of incorporating survivability considerations into conceptual design: (1) the lack of survivability of the designs located along the traditional Pareto front of lifecycle cost and mission utility, and (2) the tremendous variation in the survivability of the baseline system concepts before the addition of survivability design variables to the design vector. The first trend suggests that traditional implementations of tradespace exploration (which focus on selecting a small number of technically diverse systems located along the Pareto front for more-detailed design activities) will exclude survivable alternatives from subsequent analysis. The second trend suggests that survivability may be incorporated more effectively at the architecture-level rather than as an additive feature to a baseline system concept. Taken together, these trends indicate that delaying survivability analysis until detailed design may lead to globally suboptimal trades among cost, utility, and survivability. Conversely, the survivability tear tradespaces may be used to conduct integrated trade-offs along the Pareto efficient surface of cost, utility, and survivability.

Affordably addressing survivability requires a heterogeneous approach to eliminating, resisting, and accommodating disturbances.

To reduce the architectural fragilities in complex engineering systems, designers should embrace a portfolio of behavioral and structural strategies that reflect the diversity of the environmental disturbances they must mitigate. Just as disturbances vary in type, magnitude, and frequency, the effectiveness of alternative survivability approaches varies across systems in terms of monetary costs, performance penalties, and survivability benefits. The incorporation of survivability analysis into tradespace exploration allows the sensitivity of alternative designs and survivability strategies to be evaluated in terms of stakeholder value, allowing the identification of systems that maintain dynamic relevance through hostile contexts.

9.3. Concluding Thought

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

Glossary

architecture	the structure of components, their relationships, and the principles and guidelines governing their design and evolution over time (DoD 2003a)
attribute	decision-maker-perceived metrics that measure how well decision-maker-defined objectives are met (Ross 2003)
decision-maker	a stakeholder with control over system development resources
design	[V] the process of devising a system, component or process to meet desired needs....[includes] the establishment of objectives and criteria, synthesis, analysis, construction, testing, and evaluation (Accreditation Board for Engineering and Technology) [N] the detailed formulation of the plans or instructions for making a defined system element (Maier and Rechtin 2002)
design variables	designer-controlled quantitative parameters that reflect aspects of a concept, which taken together as a set uniquely define a system architecture (Ross 2003)
epoch	a scenario in which constraints, design concepts, available technology, and articulated attributes remain fixed (Ross 2006)
era	a set of ordered epochs (Ross 2006)
-ilities	temporal system properties that specify the degree to which systems are able to maintain or even improve function in the presence of change
reliability	the probability of functioning for a prescribed time under stipulated environmental conditions (Leveson 1995)
resilience	the ability of a system to recover from disturbance-induced value losses within a permitted recovery time
robustness	insensitivity of system value delivery to changing contexts
safety	freedom from accidents or losses (Leveson 1995)
security	protection of a system's informational, operational, and physical elements from malicious intent (Laracy and Leveson 2007)
stakeholder	an entity with interests in the outcome of a system development

survivability	the ability of a system to mitigate the impact of a finite-duration disturbance on value delivery
susceptibility	the likelihood or magnitude of a disturbance occurring within a system boundary
system-of-systems	a synergistic configuration of systems in which constituent systems are independently managed and operated (Maier 1998)
SoS engineering	the process of planning, analyzing, organizing, and integrating the capabilities of a mix of existing and new systems, with an emphasis on discovering, developing, and implementing standards that promote interoperability among systems developed via different sponsorship, management, and primary acquisition processes (AFSAB 2005)
systems engineering	the art and science of developing an operable system capable of meeting requirements within imposed constraints (Griffin 2007)
tradespace	the space spanned by an enumerated set of design variables
utility	an ordinal metric for specifying stakeholder benefit
value	a subjective measure of benefit from a bundle of consequences that is specified by a stakeholder (Keeney 1992); benefit at cost
vulnerability	the sensitivity of system value delivery to disturbance-induced losses

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.*

ACC (1996). "Multi-Command Handbook on F-16 Combat Aircraft Fundamentals." *Air Combat Command (ACC).*

AFSAB (2005). "Report on Systems-of-Systems Engineering for Air Force Capability Development." *United States Air Force Scientific Advisory Board, SAB-TR-05-04, July 2005.*

Ahmed-Zaid, F., P. Ioannou, K. Gousman and R. Rooney (1991). "Accommodation of Failures in the F-16 Aircraft Using Adaptive Control." *IEEE Control Systems Magazine*, 11(1): 73-78.

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.

Anderson, T. and J. Williamsen (2007). "Force Protection Evaluation for Combat Aircraft Crews." *48th AIAA Structures, Structural Dynamics, and Materials Conference*, Honolulu, HI.

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.

Badhwar, G. and P. Anz-Meador (1989). "Determination of the Area and Mass Distribution of Orbital Debris Fragments." *Earth, Moon, and Planets,* 45: 29-51.

Baldwin, K., M. Komaroff and P. Croll (2006). "Systems Assurance - Delivering Mission Success in the Face of Developing Threats." *A White Paper from NDIA Systems Assurance Committee.*

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

Ball, R. and D. Atkinson (1995). "A History of the Survivability Design of Military Aircraft." *36th AIAA Structures, Structural Dynamics and Materials Conference*, New Orleans, LA.

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

Ball, R. and M. Kolleck (2000). "Survivability: It's Not Just for Aircraft Anymore." *Aircraft Survivability,* Winter 2000: 10-11.

Ballhaus, W. (2005). "Successes and Challenges in Transforming National Security Space." *43rd Aerospace Sciences Meeting*, Reno, NV.

Baran, P. (1964). <u>On Distributed Communications</u>. Santa Monica, CA, RAND Corporation.

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

Bedford, T. and R. Cooke (2001). Probabilistic Risk Analysis: Foundations and Methods. Cambridge, Cambridge University Press.

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

Black, M. (2000). "Directed Energy Attack on Spacecraft." *Aircraft Survivability,* Winter 2000: 12-13.

Blaha, G., T. Pendergraft and F. Riley (2007). "Exploring Architectural Options for a Space Based Missile Defense Layer." *AIAA Space 2007*, Long Beach, CA.

Blair, B. (1985). Strategic Command and Control: Redefining the Nuclear Threat. Washington D.C., Brooking Institution Press.

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

Blaylock, J. and D. Swihart (1997). "Application of Advanced Safety Technique to Critical Subsystem Integration." *AIAA Guidance, Navigation, and Control Conference*, New Orleans, LA.

Bogdanoff, J. and F. Kozin (1985). Probabilistic Models of Cumulative Damage. New York, Wiley.

Bowley, D. and S. Lovaszy (1999). "Use of Combat Simulations and Wargames in Analytical Studies." *Proceedings of SimTecT 99*, Paper 11.

Bracken, P. (1983). The Command and Control of Nuclear Forces. New Haven, Yale University Press.

Brown, O. (2007). "Speech by Dr. Owen Brown on Fractionated Spacecraft." *DARPATech Symposium*. Anaheim, CA.

Brynestad, M. and P. Newberry (1992). "An Assessment of Combat Survivability Enhancements by Taguchi Methods." *AIAA Aircraft Design Systems Meetings*, Hilton Head, SC.

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

Canavan, G. (1991). "Notes on Space, Satellites, and Survivability." *Los Alamos National Laboratory.* LA-11847-MS, 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.

Carlson, J. and J. Doyle (2000). "Highly Optimized Tolerance: Robustness and Design in Complex Systems." *Physical Review Letters,* 84(11): 2529-2532.

Carter, A. and W. Perry (2001). Countering Asymmetric Threats. Keeping the Edge: Managing Defense for the Future. A. Carter and J. White. Cambridge, The MIT Press.

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.

CBO (2007). "Alternatives for Military Space Radar." *Congressional Budget Office.*

Cebrowski, A. and J. Raymond (2005). "Operationally Responsive Space: A New Defense Business Model." *Parameters,* Summer 2005.

Chang, C. and P. Bender (2005). "Global Hawk Integrated Sensors Suite: Recent Upgrades and Images." *InfoTech @ Aerospace*, Arlington, VA.

Chen, P. and J. Clothier (2003). "Advancing Systems Engineering for Systems-of-Systems Challenges." *Systems Engineering,* 6(3): 170-183.

Clark, C. (2008). "Space Radar is Canceled." *Space News*, 06 March, 2008.

Clausing, D. and D. Frey (2005). "Improving System Reliability by Failure-Mode Avoidance Including Four Concept Design Strategies." *Systems Engineering,* 8(3): 245-261.

Comparetto, G. and N. Hulkower (1994). "Global Mobile Communications: A Review of Three Contenders." *AIAA 15th International Communications Satellite Systems Conference*, San Diego, CA.

Corcoran, K. (2000). "Higher Eyes in the Sky: The Feasibility of Moving AWACS and JSTARS Functions into Space." Masters Thesis, School of Advanced Airpower Studies, Air University, Maxwell Air Force Base, AL.

Covault, C. (2007). "Space Control: Chinese anti-satellite weapon test will intensify funding and global policy debate on the military uses of space." *Aviation Week and Space Technology*, 22 January 2007, pp. 24-25.

Crawley, E., O. de Weck, S. Eppinger, C. Magee, J. Moses, W. Seering, J. Schindall, D. Wallace and D. Whitney (2004). "The Influence of Architecture in Engineering Systems." *MIT Engineering Systems Symposium*, Cambridge, MA.

Critchlow, R. (2006). "Nuclear Command and Control: Current Programs and Issues." *Congressional Research Service.*

Cross, N. and A. Cross (1998). "Expertise in Engineering Design." *Research in Engineering Design,* 10(3): 141-149.

Crossley, W. and D. DeLaurentis (2006). "Methods for Designing, Planning and Operating Systems of Systems." *Workshop Proceedings, Purdue University.* West Lafayette, IN.

CRS (2004). "Military Role in Space Control: A Primer." *Congressional Research Service.*

Csere, C. (2000). "Pit-Stop Precision for Army Platoons." *Car and Driver*, February 2000.

Darwin, C. (1859). On the Origin of Species. London, UK, John Murrary.

Davis, M. (1999). "Technology Challenges in Affordable Space Based Radar." *AIAA Space Technology Expo*, Albuquerque, NM.

Davis, M. (2003). "Future Space based Radar Technology Needs for Surveillance." *AIAA/ICAS International Air and Space Symposium*, Dayton, OH.

de Neufville, R. (1990). Applied Systems Analysis: Engineering Planning and Technology Management. New York, McGraw-Hill.

de Peuter, W., G. Visentin and W. Fehse (1994). "Satellite Servicing in GEO by Robotic Servicing Vehicle." *ESA Bulletin,* Issue 78: pp. 33-39.

de Weck, O., R. de Neufville and M. Chaize (2004). "Staged Deployment of Communications Satellite Constellations in Low Earth Orbit." *Journal of Aerospace Computing, Information, and Communication,* 1(3): 119-136.

DeBlois, B. (2004). "Space Weapons: Crossing the U.S. Rubicon." *International Security,* 29(2): 50-84.

DeLap, R. (1999). "Recent and Current Air Force Space Based Radar Efforts." *IEEE Aerospace Conference*, Aspen, CO.

DeLap, R. and S. Suhr (1996). "Transition of Airborne Surveillance/Reconnaissance to Space." *AIAA Space Programs and Technologies Conference*, Huntsville, AL.

Derleth, J. (2003). "Multi-Attribute Tradespace Exploration and Its Application to Evolutionary Acquisition." Master's thesis, Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, MA.

Diller, N. (2002). "Utilizing Multiple Attribute Tradespace Exploration with Concurrent Design for Creating Aerospace Systems Requirements." Master's thesis, Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, MA.

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.

DoD (2003a). "Department of Defense Architecture Framework: Version 1.0." *DoD Architecture Framework Working Group.*

DoD (2003b). "DoD Instruction 5000.2 - Operation of the Defense Acquisition System." 12 May 2003.

DoD (2004). "NSS 03-01 - National Security Space Acquisition Policy." 27 December 2004.

DoD (2007a). "Plan for Operationally Responsive Space: A Report to Congressional Defense Committees." *National Security Space Office, Department of Defense*. Washington, DC.

DoD (2007b). "System of Systems - Systems Engineering Guide." Director, Systems and Software Engineering; Deputy Undersecretary of Defense (Acquisition and Technology).

Dorr, R. (1991). "F-16 Fighting Falcon." *World Airpower Journal,* 5(Spring 1991): 50-111.

Dotseth, W. (1997). "Survivability, Safety and Reliability Analyses Integration Process." *AIAA and SAE World Aviation Congress*, Anaheim, CA.

Duren, R. (2004). "Validation and Verification of Deep-Space Missions." *Journal of Spacecraft and Rockets,* 41(4): 651-658.

Dyer, J., P. Fishburn, R. Steuer, J. Wallenius and S. Zionts (1992). "Multiple Criteria Decision Making, Multiattribute Utility Theory: The Next Ten Years." *Management Science,* 38(5): 645-654.

Eisner, H., J. Marciniak and R. McMillan (1991). "Computer-Aided System of Systems (S2) Engineering." *IEEE*

Conference on Systems, Man, and Cybernetics, Charlottesville, VA.

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*.

Flagg, S., R. White and R. Ewart (2007). "Operationally Responsive Space Specifications and Standards: An Approach to Converging with the Community." *AIAA Space 2007*, Long Beach, CA.

Fossa, C., R. Raines, G. Gunsch and M. Temples (1998). "A Performance Analysis of the IRIDIUM Low Earth Orbit Satellite System with a Degraded Satellite Constellation." *Mobile Computing and Communications Review* 2(4): 54-61.

Fovino, I. and M. Masera (2006). "Emergent Disservices in Interdependent Systems and System-of-Systems." *IEEE Conference on Systems, Man, and Cybernetics*, Taipei, Taiwan.

Fram, B. (2007). "The Case for Operationally Responsive Space." *5th Responsive Space Conference*, Los Angeles, CA.

Frey, D. and C. Dym (2006). "Validation of Design Methods: Lessons from Medicine." *Research in Engineering Design,* 17: 45-57.

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

Fulghum, D. (2007). "Hostile Atmosphere: Radiation Hardening of Microelectronics Emerging as Must-Have Protection." *Aviation Week and Space Technology*, 28 May 2007, pp. 70-71.

Futron (2002). "Launch Activity and Orbital Debris Mitigation." Second Quarter Launch Report.

Galabova, K. (2004). "Architecting a Family of Space Tugs Based on Orbital Transfer Mission Scenarios." Master's thesis, Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, MA.

Galabova, K., G. Bounova, O. de Weck and D. Hastings (2003). "Architecting a Family of Space Tugs Based on Orbital Transfer Mission Scenarios." *AIAA Space 2003*, Long Beach, CA.

GAO (2002). "Critical Infrastructure: Commercial Satellite Security Should Be More Fully Addressed." *Report to U.S. Senate, Government Accounting Office*.

GAO (2006). "Space Acquisitions: DoD Needs a Departmentwide Strategy for Pursuing Low-Cost, Responsive Tactical Space Capabilities." *U.S. Government Accountability Office*. Report to the Chairman, Subcommittee on Strategic Forces, Committee on Armed Services, House of Representatives, GAO-06-449, March 2006.

Garrison, T., J. Pizzicaroli and P. Swan (1997). "Systems Engineering Trades for the IRIDIUM Constellation." *Journal of Spacecraft and Rockets,* 34(5): 675-680.

Giffen, R. (1982). "US Space System Survivability: Strategic Alternatives for the 1990s." *National Defense University Press*. National Security Affairs Monograph Series 82-4, Washington, DC.

Gigerenzer, G. and D. Goldstein (1996). "Reasoning the Fast and Frugal Way: Models of Bounded Rationality." *Psychological Review,* 103(4): 650-669.

Gonzales, D. (1999). The Changing Role of the U.S. Military in Space. Santa Monica, RAND.

Graves, R. (2002). "Space Station Meteoroid and Orbital Debris Survivability." *43rd AIAA Structures, Structural Dynamics, and Materials Conference*, Denver, CO.

Griffin, M. (2007). "Systems Engineering and the Two Cultures of Engineering." *Boeing Lecture, Purdue University.*

Gruhl, W. (1992). "Lessons Learned, Cost/Schedule Assessment Guide." *Internal presentation*, NASA Comptroller's Office.

Haffa, R. and J. Patton (1998). "Gaming the System of Systems." *Parameters,* Spring 1998: 110-121.

Hall, D. (2004). "Integrated Survivability Assessment (ISA) in the Acquisition Lifecycle." *45th AIAA Structures, Structural Dynamics, and Materials Conference*, Palm Springs, CA.

Harper, M., M. Thornton and S. Szygenda (2007). "Disaster Tolerant Systems Engineering for Critical Infrastructure Protection." *1st IEEE Systems Conference*, Honolulu, HI.

Hastings, D. (2004). "The Future of Engineering Systems: Development of Engineering Leaders." *MIT Engineering Systems Symposium*, Cambridge, MA.

Hastings, D. and H. Garrett (1996). Spacecraft-Environment Interactions. New York, Cambridge University Press.

Hazelrigg, G. (1996). Systems Engineering: An Approach to Information-Based Design. Upper Saddle River, Prentice Hall.

Hazelrigg, G. (2003). "Validation of Engineering Design Alternative Selection Methods." *Engineering Optimization,* 35(2): 103-120.

He, Y. and H. Zhao (2007). "Survivability Performance Evaluation for Satellite Communication Network Based on Walker Constellation." *SPIE Conference on Space Information Technology*, Wuhan, China.

Hehs, E. (1999). "F-16 Refresher Course." *Code One: An Airpower Projection Magazine*, April 1999.

Herscovitz, J. and D. Barnett (2007). "Decision Analysis for Design Trades for a Combined Scientific-Technological Mission Orbit on Venus Micro Satellite." *17th INCOSE Symposium*, San Diego, CA.

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.

Hillier, F. and G. Lieberman (1995). Introduction to Operations Research. New York, McGraw-Hill.

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

Hopkins, A. (1971). "A Fault-Tolerant Information Processing Concept for Space Vehicles." *IEEE Transactions on Computers,* 20(11): 1394-1403.

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

Iannotta, B. (2009). "Iridium Satellite Lost in Collision." *Space News*, 11 February 2009.

Iovanov, M., S. Schulz, G. Dixon, A. Puderbaugh and R. Shepperd (2003). "Automation of Daily Tasks Necessary for the Management of a Large Satellite Constellation." *AIAA Space 2003*, Long Beach, CA.

Isakowitz, S., J. Hopkins and J. P. Hopkins (2004). International Reference Guide to Space Launch Systems. Reston, American Institute of Aeronautics and Astronautics.

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

Jilla, C. (2002). "A Multiobjective, Multidisciplinary Design Optimization Methodology for the Conceptual Design of Distributed Satellite Systems." Doctoral dissertation, Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, MA.

Johannesson, M. (1995). "The Ranking Properties of Healthy-Years Equivalents and Quality Adjusted Life-Years Under Certainty and Uncertainty." *International Journal of Technology Assessment in Health Care,* 11(1): 40-48.

Johnson, S. (1997). "Three Approaches to Big Technology: Operations Research, Systems Engineering, and Project Management." *Technology and Culture,* 38(4): 891-919.

Joseph, R. (2006). "The U.S. National Space Policy." *The George Marshall Institute*. Washington, D.C.

JTCG/AS (2001). Aerospace Systems Survivability Handbook. Arlington, VA, Joint Technical Coordinating Group on Aircraft Survivability.

Jugulum, R. and D. Frey (2007). "Toward a Taxonomy of Concept Designs for Improved Robustness." *Journal of Engineering Design,* 18(2): 139-156.

Karpiscak, J. (1998). "Proliferation of Commercial Space Systems - Benefits and Concerns for U.S. Combat Operations." *AIAA Defense and Civil Space Programs Conference*, Huntsville, AL.

Kean, T., L. Hamilton, R. Ben-Veniste, B. Kerrey, F. Fielding, J. Lehman, J. Gorelick, T. Roemer, S. Gorton and J. Thompson (2004). National Commission on Terrorist Attacks Upon the United States, Washington D.C.

Keeney, R. (1992). Value-Focused Thinking: A Path to Creative Decisionmaking. Cambridge, Harvard University Press.

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

Kharoufeh, J. and S. Cox (2005). "Stochastic Models for Degradation-Based Reliability." *IIE Transactions,* 37(6): 533-543.

Klinkrad, H. (2006). Space Debris Models and Risk Analysis. Chichester, Springer.

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

Kossiakoff, A. and W. Sweet (2003). Systems Engineering: Principles and Practice. Hoboken, John Wiley and Sons.

Lai, S., E. Murad and W. McNeil (2002). "Hazards of Hypervelocity Impacts on Spacecraft." *Journal of Spacecraft and Rockets,* 39(1): 106-114.

Lamamy, J. (2007). "Methods and Tools for the Formulation, Evaluation and Optimization of Rover Mission Concepts." Doctoral dissertation, Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, MA.

Langworthy, D. and D. Wells (1998). "Survivability is Utility." *Object Services and Consulting, Inc.*

Laracy, J. and N. Leveson (2007). "Applying STAMP to Critical Infrastructure Protection." *IEEE Conference on Technologies for Homeland Security*, Boston, MA.

Lemme, P., S. Glenister and A. Miller (1998). "Iridium Aeronautical Satellite Communications." *Digital Avionics Systems Conference*, Belleview, WA.

Leveson, N. (1995). Safeware: System Safety and Computers. Boston, Addison-Wesley.

Leveson, N. (2002). System Safety Engineering: Back to the Future. Cambridge, MIT Department of Aeronautics and Astronautics.

Leveson, N. (2004). "Role of Software in Spacecraft Accidents." *Journal of Spacecraft and Rockets,* 41(4): 564-575.

Leveson, N., M. Daouk, N. Dulac and K. Marais (2004). "A Systems Theoretic Approach to Safety Engineering." *MIT Engineering Systems Symposium*, Cambridge, MA.

Lin, J. (2009). "Exploring Flexible Strategies in Engineering Systems Using Screening Models: Applications to Offshore Petroleum Projects." Doctoral dissertation, Engineering Systems Division, Massachusetts Institute of Technology, Cambridge, MA.

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

Liou, J., M. Matney, P. Anz-Meador, D. Kessler, M. Jansen and J. Theall (2002). "The New NASA Orbital Debris Engineering Model ORDEM2000." NASA/TP-2002-210780.

Long, A., M. Richards and D. Hastings (2007). "On-Orbit Servicing: A New Value Proposition for Satellite Design and Operation." *Journal of Spacecraft and Rockets,* 44(4): 964-976.

Maier, M. (1998). "Architecting Principles for Systems-of-Systems." *Systems Engineering,* 1(4): 267-284.

Maier, M. and E. Rechtin (2002). The Art of Systems Architecting. Boca Raton, CRC Press.

Maine, K., C. Devieux and P. Swan (1995). "Overview of Iridium Satellite Network." *Wescon Application Conference*, San Francisco, CA.

March, J. and Z. Shapira (1987). "Managerial Perspectives on Risk and Risk Taking." *Management Science,* 33(11): 1404-1418.

McConnell, J. (2007). "A Life-Cycle Flexibility Framework for Designing, Evaluating and Managing "Complex" Real Options: Case Studies in Urban Transportation and Aircraft Systems." Doctoral dissertation, Engineering Systems Division, Massachusetts Institute of Technology, Cambridge, MA.

McManus, H. and D. Hastings (2006). "A Framework for Understanding Uncertainty and its Mitigation and Exploitation in Complex Systems." *IEEE Engineering Management Review,* 34(3): 81-94.

McManus, H., D. Hastings and J. Warmkessel (2004). "New Methods for Rapid Architecture Selection and Conceptual Design." *Journal of Spacecraft and Rockets,* 41(1): 10-19.

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

McManus, H. and T. Schuman (2003). "Understanding the Orbital Transfer Vehicle Tradespace." *AIAA Space 2003*, Long Beach, CA.

McManus, H. and J. Warmkessel (2004). "Creating Advanced Architectures for Space Systems: Emergent Lessons from New Processes." *Journal of Spacecraft and Rockets,* 41(1): 69-74.

McVey, M. (2002). "Valuation Techniques for Complex Space Systems: An Analysis of a Potential Satellite Servicing Market." Master's thesis, Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, MA.

Moitra, S. and S. Konda (2000). "A Simulation Model for Managing Survivability of Networked Information Systems." *Carnegie Mellon Software Engineering Institute.*

Moore, A. and R. Ellison (2003). "TRIAD: A Framework for Survivability Architecting." *ACM Conference on Computer and Communications Security,* Fairfax, VA.

Morring, F., A. Butler and M. Mecham (2009). "Crash Course: Iridium's loss could be a harbinger of things to come in low Earth orbit." *Aviation Week and Space Technology*, 16 February 2009, pp. 20-21.

Morris, E., P. Place, D. Smith, B. Ellison, F. Redner and C. Woody (2007). "A Framework for Analysis of Mission Survivability within Dynamic Environments." *AIAA Infotech@Aerospace*, Rohnert Park, CA.

Moses, J. (2004). "Foundational Issues in Engineering Systems: A Framing Paper." *MIT Engineering Systems Symposium*, Cambridge, MA.

Mowthorpe, M. (2002). "US Military Space Policy 1945-92." *Space Policy,* 18(1): 25-36.

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

NASA (2007). "NASA Systems Engineering Handbook." NASA/SP-2007-6105.

Neuman, W. (2006). Social Research Methods. Boston, Pearson.

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

Nilchiani, R. and D. Hastings (2007). "Measuring the Value of Flexibility in Space Systems: A Six-Element Framework." *Systems Engineering,* 10(1): 26-44.

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.

NRC (2006). Future Air Force Needs for Survivability. Washington, DC, The National Academy Press.

NTIA (1996). "Federal Standard 1037C." National Telecommunications and Information Administration.

O'Hanlon, M. (2004). Neither Star Wars Nor Sanctuary: Constraining the Military Uses of Space. Washington D.C., Brookings Institution Press.

Osinga, F. (2006). Science, Strategy and War: The Strategic Theory of John Boyd. London, UK, Routledge.

Pate-Cornell, M., R. Dillon and S. Guikema (2004). "On the Limitations of Redundancies in the Improvement of System Reliability." *Risk Analysis,* 24(6): 1423-1436.

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

Perrow, C. (1999). Normal Accidents: Living with High-Risk Technologies. Princeton, Princeton University Press.

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

Pike, J. (1986). "Will "Star Wars" Work." *Annals of the New York Academy of Sciences,* 489: 83-93.

Pillai, S., K. Li and B. Himed (2008). Space Based Radar: Theory and Applications. New York, McGraw-Hill.

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

Pizzicaroli, J. (1997). "Launching and Building the IRIDIUM Constellation." *Mission Design and Implementation of Satellite Constellations*, Toulouse, France.

Post, J., M. Bennett and R. Hall (2006). "The Cost and Effectiveness of Alternative Space Radar Constellations." *AIAA Space 2006*, San Jose, CA.

Pratt, S., R. Raines, C. Fossa and M. Temple (1999). "An Operational and Performance Overview of the IRIDIUM Low Earth Orbit Satellite System." *IEEE Communications Surveys*, Second Quarter 1999, 2-10.

Pratt, T., C. Bostian and J. Allnutt (2003). Satellite Communications. Hoboken, John Wiley & Sons.

Preiss, B., S. Fiedler and T. Kellett (1999). "Space Based Radar Analysis within the Spacecraft Simulation Toolkit." *AIAA Space Technology Conference*, Albuquerque, NM.

Puderbaugh, A., G. Dixon, L. Shroyer and W. Boyce (2002). "A Global and Local History of Drag Effects at Iridium Mission Altitude." *AIAA Astrodynamics Specialist Conference*, Monterey, CA.

Rajan, P., M. Van Wie, M. Campbell, K. Wood and K. Otto (2005). "An Empirical Foundation for Product Flexibility." *Design Studies,* 26(4): 405-438.

Rance, M. (2007). "Missile Defence and Space." *AIAA Space 2007*, Long Beach, CA.

Remo, J. (2005). "Orbital Debris Effects from Space-Based Ballistic Missile Interception." *Journal of Spacecraft and Rockets,* 42(3): 487-492.

Rhodes, D. (2004). "Report on Air Force/LAI Workshop on Systems Engineering for Robustness." Arlington, VA.

Rhodes, D. and D. Hastings (2004). "The Case for Evolving Systems Engineering as a Field within Engineering Systems." *MIT Engineering Systems Symposium*, Cambridge, MA.

Richards, M. (2006). "On-Orbit Serviceability of Space System Architectures." Dual Master's thesis, Department of Aeronautics and Astronautics and Engineering Systems Division, Massachusetts Institute of Technology, Cambridge, MA.

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

Richards, M., P. Springmann and M. McVey (2005). "Assessing the Challenges to a Geosynchronous Space Tug System." *SPIE Defense and Security Symposium*, Orlando, FL.

Roberts, C. (2003). "Architecting Evolutionary Strategies Using Spiral Development for Space Based Radar." Technology and Policy Program, Massachusetts Institute of Technology, Cambridge, MA.

Roos, D. (2004). "Engineering Systems at MIT - The Development of the Engineering Systems Division." *MIT Engineering Systems Symposium*, Cambridge, MA.

Rosenwald, M. (2007). "Downside of Dominance? Popularity of Lockheed Martin's F-16 Makes Its F-35 Stealth Jet a Tough Sell." *Washington Post*, 17 December 2007.

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

Ross, A. and D. Hastings (2005). "The Tradespace Exploration Paradigm." *15th INCOSE Symposium*, Rochester, NY.

Ross, A. and D. Hastings (2006). "Assessing Changeability in Aerospace Systems Architecting and Design Using Dynamic Multi-Attribute Tradespace Exploration." *AIAA Space 2006*, San Jose, CA.

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.

Ross, A., H. McManus, A. Long, M. Richards, D. Rhodes and D. Hastings (2008). "Responsive Systems Comparison Method: Case Study in Assessing Future Designs in the Presence of Change." *AIAA Space 2008*, San Diego, CA.

Ross, A. and D. Rhodes (2008). "Using Natural Value-Centric Time Scales for

Conceptualizing System Timelines Through Epoch-Era Analysis." *18th INCOSE Symposium*, Utrecht, Netherlands.

Ross, A., D. Rhodes and D. Hastings (2008). "Defining Changeability: Reconciling Flexibility, Adaptability, Scalability, Modifiability, and Robustness for Maintaining System Lifecycle Value." *Systems Engineering,* 11(4): 246-262.

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."

Ryan, A. (2006). "About the Bears and the Bees: Adaptive Responses to Asymmetric Warfare." *6th International Conference on Complex Systems*, Boston, MA.

Sage, A. and C. Cuppan (2001). "On the Systems Engineering and Management of Systems of Systems and Federations of Systems." *Information, Knowledge, Systems Management,* 2(4): 325-345.

Saleh, J., J. Torres-Padilla, D. Hastings and D. Newman (2006). "To Reduce or to Extend a Spacecraft Design Lifetime?" *Journal of Spacecraft and Rockets,* 43(1): 207-217.

SecAF (1994). "System Survivability, Air Force Instruction 62-201." Washington DC.

Shah, N. (2004). "Modularity as an Enabler for Evolutionary Acquisition." Master's thesis, Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, MA.

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.

Shellans, M. and W. Matoush (1992). "Designing Survivable Space Systems." *Aerospace America*, 38.

Siddiqi, A. and O. De Weck (2006). "Self-Similar Modular Architectures for Reconfigurable Space Systems." *57th International Astronautical Congress*, Valencia, Spain.

Silver, M. and O. de Weck (2007). "Time-Expanded Decision Networks: A Framework for Designing Evolvable Complex Systems." *Systems Engineering,* 10(2): 167-186.

Simon, H. (1996). The Sciences of the Artificial. Cambridge, The MIT Press.

Singer, J. (2004). "Congress Guts Space Radar, Trims Communications Programs." *Space News*, 21 July, 2004.

Singh, A. and C. Dagli (2007). "Incorporating Security and Survivability into System of Systems Architecting." *17th INCOSE Symposium*, San Diego, CA.

Smallwood, W. (1993). Warthog: Flying the A-10 in the Gulf War. Dulles, Potomac Books.

Soban, D. and D. Mavris (2000). "Methodology for Assessing Survivability Tradeoffs in the Preliminary Design Process." *2000 World Aviation Conference*, San Diego, CA.

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.

Spires, D. (2001). Horizons: A Half Century of Air Force Space Leadership. Maxwell Air Force Base, Air University Press.

Stagney, D. (2003). "The Integrated Concurrent Enterprise." Dual Master's thesis, Department of Aeronautics and Astronautics, Sloan School of Management, Massachusetts Institute of Technology, Cambridge, MA.

Stares, P. and J. Pike (1985). "The 'Star Wars' Initiative." *Space Policy,* 1(2): 153-163.

Stenger, D. (1996). "Survivability Analysis of the Iridium Low Earth Orbit Satellite Network." Master's thesis, Department of Electrical and Computer Engineering, Air Force Institute of Technology, Wright-Patterson Air Force Base, OH.

Sterman, J. (2000). Business Dynamics: Systems Thinking and Modeling for a Complex World. Boston, McGraw-Hill.

Suh, E. (2005). "Flexible Product Platforms." Doctoral dissertation, Engineering Systems Division, Massachusetts Institute of Technology, Cambridge, MA.

Sullivan, B. (2005). "Technical and Economic Feasibility of Telerobotic On-Orbit Satellite Servicing." Doctoral dissertation, Department of Aerospace Engineering, University of Maryland, College Park, MD.

Swan, P. (1997). "A Revolution in Progress: IRIDIUM LEO Operations." *AIAA Defense and Space Programs Conference,* Huntsville, AL.

Swinerd, G., H. Lewis, N. Williams and C. Martin (2003). "Self-Induced Collision Hazard in High and Moderate Inclination Satellite Constellations." *Acta Astronautica,* 54(3): 191-201.

Tang, V. (2006). "Corporate Decision Analysis: An Engineering Approach." Doctoral dissertation, Engineering Systems Division, Massachusetts Institute of Technology, Cambridge, MA.

Thomas, S., H. Kwatny, B. Chang and C. Belcastro (2005). "Regulator Design for Control Surface Failure Accommodation in an F-16." *AIAA Guidance, Navigation, and Control Conference*, San Francisco, CA.

Thomson, A. (1995). "Satellite Vulnerability: A Post-Cold War Issue?" *Space Policy,* 11(1): 19-30.

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

Thurston, D. (1990). "Multiattribute Utility Analysis in Design Management." *IEEE Transactions on Engineering Management,* 37(4): 296-301.

Tirpak, J. (2002). "The Space Based Radar Plan." *Air Force Magazine,* August 2002: 63-66.

Tomme, E. (2006). "The Strategic Nature of the Tactical Satellite." *Airpower Research Institute, Airpower University.*

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

Tversky, A. and D. Kahneman (1974). "Judgment Under Uncertainty: Heuristics and Biases." *Science,* 185(4157): 1124-1131.

U.S. (2006). "U.S. National Space Policy." *White House Office of Science and Technology Policy*, Released 31 August 2006, Washington, D.C.

UCS (2006). "Union of Concerned Scientists Satellite Database."

Ulrich, K. and S. Eppinger (2004). Product Design and Development. Boston, McGraw Hill.

UN (1999). "Technical Report on Space Debris."

USA (2006). "The UH-60A Black Hawk." *U.S. Army Aviation Warfighting Center.*

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

USAF (2007). "A-10/OA-10 Thunderbolt II." *Air Force Fact Sheet.*

Valerdi, R. and H. Davidz (2007). "Empirical Research in Systems Engineering: Challenges and Opportunities of a New Frontier." *5th Conference on Systems Engineering Research*, Hoboken, NJ.

Van Kasteren, J. (2004). "Micro Satellite Swarm Reduces Vulnerability." Delft Outlook.

von Neumann, J. and O. Morgenstern (1953). Theory of Games and Economic Behavior. Princeton, Princeton University Press.

Wang, T. (2005). "Real Options "in" Projects and Systems Design: Identification of Options and Solution for Path Dependency." Doctoral dissertation, Engineering Systems Division, Massachusetts Institute of Technology, Cambridge, MA.

Webster, M. (2008). Webster's New World College Dictionary. Cleveland, Wiley.

Weigel, A. (2002). "Bring Policy into Space Systems Conceptual Design: Qualitative and Quantitative Methods." Doctoral dissertation, Engineering Systems Division, Massachusetts Institute of Technology, Cambridge, MA.

Weigel, A. and D. Hastings (2004). "Measuring the Value of Designing for Future Downward Budget Instabilities." *Journal of Spacecraft and Rockets,* 41(1): 111-119.

Wertz, J. (2006). "Expected Productivity-Based Risk Analysis in Conceptual Design: With Application to the Terrestrial Planet Finder Interferometer Mission." Doctoral dissertation, Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, MA.

Wertz, J. and W. Larson (1999). Space Mission Analysis and Design. El Segundo, Microcosm Press.

Wertz, J. and D. Miller (2005). "Expected Productivity-Based Risk Analysis in Conceptual Design." *56th International Astronautical Congress*, Fukuoka, Japan.

Wheelon, A. (1965). "Vulnerability of the CORONA System to Soviet Countermeasures." Memo to the Director of Central Intelligence, 16 September 1965.

Wheelon, A. (1986). "Antisatellite Weapons and Space Warfare." *Annals of the New York Academy of Sciences,* 489: 38-47.

Wheelon, A. (1997). "CORONA: The First Reconnaissance Satellites." *Physics Today*, February 1997, pp. 24-30.

Wickert, D., G. Shaw and D. Hastings (1998). "Impact of a Distributed

Architecture for Space-Based Radar." *Journal of Spacecraft and Rockets,* 35(5): 703-713.

Wiedemann, C., M. Oswald, S. Stabroth, D. Alwes and P. Vorsmann (2008). "Cost and Benefit of Satellite Shielding." *Acta Astronautica,* 63: 136-145.

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.

Wilson, T. (2001). "Threats to United States Space Capabilities." prepared for the Commission to Assess United States National Security Space Management and Organization, January 2001.

Wright, D., L. Grego and G. Lisbeth (2005). "The Physics of Space Security: A Reference Manual." *American Academy of Arts and Sciences*. Cambridge.

Young, T., D. Hastings and W. Schneider (2003). "Report of the Defense Science Board / Air Force Scientific Advisory Board Joint Task Force on Acquisition of National Security Space Programs." *Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics*. Washington, DC.

Yurick, W. and D. Doss (2002). "A Survivability-Over-Security (SOS) Approach to Holistic Cyber-Ecosystem Assurance." *IEEE Workshop on Information Assurance*, United States Military Academy, West Point, NY.

Zinn, A. (2004). "The Use of Integrated Architectures to Support Agent Based Simulation: An Initial Investigation." Master's thesis, Department of Aeronautics and Astronautics, Air Force Institute of Technology, Wright-Patterson Air Force Base, OH.

Appendix A. A-10A Design Principles

The A-10 "Warthog" is a single-seat, twin-engine combat aircraft used by the U.S. Air Force (USAF) to provide close air support for ground forces. Equipped with 16,000 pounds of mixed ordnance, including a 30-mm gun and air-to-surface missiles, the primary mission of the A-10 is to attack tanks and other armored vehicles. As documented in Ball (2003), the motivation for developing the A-10 stems from the United States experience in the Vietnam War during which approximately 5000 aircraft—nearly equally divided between fixed-wing aircraft and helicopters—were lost. A large number of these aircraft were brought down by small arms fire, surface-to-air missiles, and low level anti-aircraft fire—indicating the need for reducing the vulnerability of future aircraft. To fill the need for survivable long-loiter aircraft for close air support, the A-10 was developed as a heavily armored aircraft incorporating over 100 vulnerability reduction features (Ball and Atkinson 1995). In doing so, the A-10 became the first USAF aircraft to be designed exclusively for the close air support mission as well as the first modern fixed-wing aircraft to be designed (from its inception) to a complete set of survivability requirements.

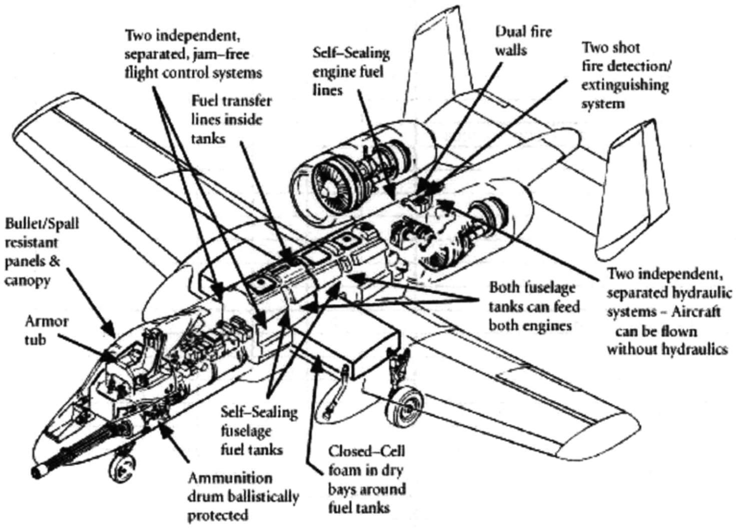

Two independent, separated, jam-free flight control systems
Self-Sealing engine fuel lines
Dual fire walls
Two shot fire detection/ extinguishing system
Fuel transfer lines inside tanks
Bullet/Spall resistant panels & canopy
Armor tub
Both fuselage tanks can feed both engines
Two independent, separated hydraulic systems - Aircraft can be flown without hydraulics
Self-Sealing fuselage fuel tanks
Closed-Cell foam in dry bays around fuel tanks
Ammunition drum ballistically protected

Figure 9-1. Some Vulnerability Reduction Features on the A-10A Thunderbolt II (Ball 2003)

Since its delivery to the USAF in 1977, the survivability of the A-10 has been validated through its extensive combat experiences, including the first and second Persian Gulf Wars, Kosovo, and Afghanistan (Ball 2003; USAF 2007). Among other attributes noted in the USAF fact sheet, "the aircraft can survive direct hits from armor-piercing and high explosive projectiles up to 23mm" into the "titanium bathtub" within which the pilot sits. The ability of the A-10 to absorb a gross amount of punishment was proven in the first Persian Gulf War. Flying an average of 193 missions per day for 42 days, the A-10 destroyed half of the armor in two Iraqi Republican Guard divisions while losing only six A-10 aircraft and two pilots (Smallwood 1993). Figure 9-1 illustrates some of the vulnerability reduction features incorporated into the A-10: self-sealing fuel tanks to prevent fires, explosions, and fuel supply depletion; redundant flight control, hydraulic, and fuel tank systems; and other features.

In selecting the A-10, the unit of analysis is a piloted aircraft operating in a hostile combat environment (*e.g.*, confronting guns and missiles carried by enemy air and ground systems). The required value threshold for the system is a safe and successful completion of a given mission. The emergency value threshold is met if the crew and vehicle are able to exit the combat zone despite a failure to achieve mission objectives. Survivability features may add value over the entire lifecycle of a given disturbance (*i.e.*, Epoch 1a, Epoch 2 and Epoch 1b).

Table 9-1. Tracing of A-10A "Warthog" Survivability Features to Design Principles

		Design Principles											
		Type I						Type II				Type III	
	A-10A: Sample Survivability Features	prevention	mobility	concealment	deterrence	preemption	avoidance	hardness	evolution	redundancy	diversity	replacement	repair
structure	redundant primary structure									X			
	dual vertical stabilizers to shield heat exhaust			X									
	long low-set wings (flight possible even if missing 1/2 wing)									X			
	interchangeable engines, landing hear, and vertical stabilizers												X
cockpit	pilot sits in a titanium/aluminum armor bathtub							X					
	spall shields between armor and pilot							X					
	bullet resistant windscreen							X					
	spall resistant canopy side panels							X					
	ACES-II ejection seat								X				
	night vision goggles for operating in darkness			X									
	situational awareness data link												
fuel system	two self-sealing fuel tanks located away from ignition sources									X	X		X
	short, self-sealing feed lines												X
	wing fuel used first								X				
	most fuel lines located inside tanks							X					
	redundant feed flow									X			
	open cell foam in all tanks							X					
	closed cell foam in dry bays around tanks							X					
	draining and vents in vapor areas	X							X				
propulsion	maneuverability at low airspeeds and altitude		X				X						
	two widely separated engines										X		
	engines mounted away from fuselage										X		
	dual fire walls							X		X			
	fail-active fire detection with two shot fire extinguishing												X
	engine case armor							X					
	separation between fuel tanks and air inlets										X		
	one engine out capability									X			
flight control	two independent, separated mechanical flight controls									X	X		
	two rudders and elevators									X			
	armor around stick where redundant controls converge							X					
	two independent, hydraulic power subsystems									X			
	manual reversion mode for flight controls									X	X		
	dual, electrically powered trim actuators									X			
	less flammable hydraulic fuel							X					
	jam-free							X					
armament	one 30 mm GAU-8/A Avenger Gatling gun	X			X	X							
	16,000 pounds of mixed ordnance	X			X	X							
	infrared countermeasure flares			X									
	electronic countermeasures chaff			X									
	jammer pods	X				X							
	illumination flares												
	AIM-9 Sidewinder air-to-air missiles	X			X	X							

Upon gathering data on 42 survivability features of the A-10 from Ball and Atkinson (1995) and the USAF Fact Sheet (2007), the features were sorted into six categories (*i.e.*, structure, cockpit, fuel system, propulsion, flight control, and armament) and traced to the twelve initial design principles. Table 9-1 presents the results of this empirical mapping. As one might expect, the density of Type II mappings is much higher than Type I mappings, strongly suggesting the emphasis designers placed on vulnerability reduction in the A-10. Not every feature contributing to the survivability of the A-10 is successfully traced to an existing design principle, and the mapping of some of the features was problematic (as noted in cells shaded grey). In the process of resolving these problem areas, potential improvements to the survivability framework, current set of design principles, and definition of certain design principles were revealed.

In the process of tracing the 42 survivability features of the A-10 to the design principles, four insights emerged. The first relates to the definition of *redundancy*. Moving down Table 9-1 to the first grey cell, one sees the survivability feature of [structure] long low-set wings (with flight possible even when missing half of a wing) intersecting with the design principle of redundancy. Redundancy, which is defined in terms of duplication of critical system components, is a poor fit for this survivability feature. Redundancy implies substitution of components to maintain a consistent level of performance whereas an ability to fly missing half of a wing is indicative of design *margin*. While redundancy and margin are related in terms of having something "extra," they are fundamentally different concepts because margin implies a continuum of capability which, if reduced, may impact end-user value. Another example in Table 9-1 of the benefit for having margin as a separate design principle is the [propulsion] one engine out capability (*i.e.*, the second engine does not provide true redundancy; rather, the propulsion system accommodates graceful degradation).

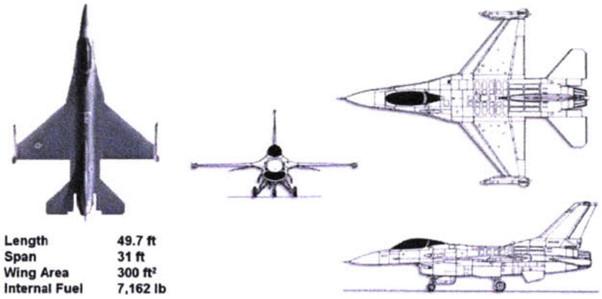
The second insight arises from eight rows down with the [cockpit] situational awareness data link feature as well as near the bottom of the matrix with the [armament] illumination flares feature. In attempting to trace situational awareness to the framework, it was not clear which design principles, if any, are employed by these features. For example, just as health monitoring is necessary to conduct effective *repair* and *replacement* activities following a disturbance, situational awareness is a prerequisite for any design principle that involves decision-making before or during a disturbance. These active design principles include *prevention*, *mobility*, *deterrence*, *preemption*, *avoidance*, and *evolution*. However, situational awareness by itself does not employ any of these principles. Rather, it is an essential activity taken by an internal system agent to inform decision-making before actions employing particular design principles are taken.

The third insight arises from a closer look at the column under the Type II survivability principle of *diversity*. As defined in the preliminary design principle set (Table 4-3), diversity is characteristic or spatial variation to limit the effectiveness of homogeneous disturbances. This is an extremely broad definition that includes variation in both the properties (*i.e.*, heterogeneity) and locations of system elements (*i.e.*, distribution). These are two fundamentally different concepts. The need for a decomposition of the diversity design principle into two separate principles such as a *heterogeneity* and *distribution* is underscored by the fact that five of the six manifestations of "diversity" in the A-10 survivability features (shaded in grey) employ distribution: [fuel system] two self-sealing fuel tanks located away from ignition sources, [propulsion] two widely separated engines, engines mounted away from fuselage, separation between fuel tanks and air inlets, and [flight control] two independent, separated mechanical flight controls.

The fourth insight gained from examining the A-10 is recognition of the distinction between physical redundancy and functional redundancy. Defined in the preliminary design principles as the duplication of system components to increase reliability, this definition was found to be inapplicable upon considering the survivability feature of [flight control] manual reversion mode of flight controls. Replacing the existing definition of redundancy (based on physical duplication) with a definition based on functional duplication would fix this problem.

Appendix B. F-16C Design Principles

The F-16 "Fighting Falcon" (Figure 9-2) is a single-engine, multirole tactical jet fighter in use by 24 nations. The F-16 platform supports more than 100 weapon and sensor systems, enabling a variety of air-to-air and air-to-ground missions. As a compact and highly maneuverable "dogfighting" aircraft, the F-16 has proven to be highly survivable with only six shootdowns in over 200,000 flown sorties. The operational experience of the F-16 (in Iraq, Afghanistan, Kosovo) and extremely low sortie loss rate affirms the survivability of the system to its specified combat environment. For example, only four F-16's were damaged in Operation Desert Storm despite the fact that more sorties were flown by F-16's than any other aircraft. These 13,066 sorties included attacks on airfields, military production facilities, and Scud missile sites (Ball 2003). When first introduced by the U.S. Air Force in 1978, about 1,000 F-16's were to be produced. As of today, 4,500 have been built with Lockheed Martin's backlog of 116 foreign orders scheduled to keep production running until at least 2012 (Dorr 1991; Rosenwald 2007).



Length	49.7 ft
Span	31 ft
Wing Area	300 ft²
Internal Fuel	7,162 lb

(http://www.aerospaceweb.org/question/planes/q0163.shtml)

Figure 9-2. F-16C Fighting Falcon

The experience of the U.S. Air Force in Vietnam—during which a lack of maneuverability of U.S. fighters at transonic speeds hindered performance against agile enemy fighters—was the impetus for an F-16 concept that focused on compactness and extreme maneuverability (Hehs 1999). Departing from the dominant paradigm of U.S. fighters at the time (*e.g.*, high cost, complexity, and weight of F-4 and F-111 aircraft), the F-16 was the winning design of the Lightweight Fighter Program that stressed low-cost and high procurement numbers (Dorr 1991). To achieve superior dogfighting capabilities, the F-16 design embraced many innovations: frameless bubble cockpit, fly-by-wire control system, cropped delta wings and long wing-body strakes, negative static stability, and a side-mounted control stick and reclined seat for pilot tolerance of 9-g turns.

To test the baseline set of design principles, survivability features were gathered from open-source literature on the F-16C, Block 40 Build (Ahmed-Zaid et al. 1991; Dorr 1991; ACC 1996; Blaylock and Swihart 1997; Hehs 1999; Thomas et al. 2005; Rosenwald 2007). (Block 40 F-16C's entered service in 1988 and featured an improved all-day/all weather strike capability with the LATIRN navigation pods. LATIRN includes a terrain-following radar, forward-looking infrared, and laser targeting.) In testing the design principles against the F-16, the unit of analysis is a piloted F-16C vehicle operating in a hostile combat environment (*e.g.*, confronting guns and missiles carried by enemy air and ground systems). The required value threshold for the system is a safe and successful completion of a given mission. The emergency value threshold is met if the crew and vehicle are able to exit the combat zone despite a failure to achieve mission objectives. Survivability features may add value over the entire lifecycle of a given disturbance (*i.e.*, Epoch 1a, Epoch 2 and Epoch 1b).

Upon identifying 36 survivability features of the F-16, the features were sorted into five categories (*i.e.*, structure, cockpit, propulsion, flight control, and armament) and traced to the seventeen general design principles and ODA loop. Table 9-2 presents the results of this empirical mapping. As one might expect, the density of Type I mappings is higher than Type II mappings, indicative of the emphasis that designers placed on susceptibility reduction in the F-16. The F-16 is adept at avoiding disturbances given its superior maneuverability provided by a 29,000 pound thrust engine and negative static stability. The F-16 is also able to conceal itself from enemy sensors given its compact size (*i.e.,* 50 x 31 x 16 feet) and small infrared and radio-frequency signatures. A full suite of modern threat warning systems enables active *concealment* strategies, including electronic countermeasures and chaff and flare dispensers. Many vulnerability reduction features are also incorporated into the design, such as buried fuel lines, fuel inerting systems, critical systems redundancy, fault tolerant flight control, and shielding.

Table 9-2. Tracing F-16 Survivability Features to Design Principles

		Design Principles																	
		Type I (Reduce Susceptibility)						Type II (Reduce Vulnerability)									Type III		
	F-16C: Sample Survivability Features	prevention	mobility	concealment	deterrence	preemption	avoidance	hardness	redundancy	margin	heterogeneity	distribution	reduction	fail-safe	evolution	containment	replacement	repair	ODA - exclusive
structure	small visual IR and RF signature (50 x 31 x 16 ft)			X															
	sustains 9-g turns		X				X	X											
	two-tone grey camouflage (standard)			X															
	tail and wing proximity for enhanced maneuverability		X				X												
	blended wing fuselage to reduce transonic drag		X	X			X												
cockpit	situational awareness data link																		X
	autonomous precision targeting (if necessary)	X			X	X							X						
	bubble canopy for enhanced visibility																		X
	cockpit compatibility with night vision goggles			X															
	LANTIRN navigation pod for nighttime operations			X															
	modular avionics																X	X	
	30 degree seat back angle to increase g tolerance							X											
	ACES II ejection seat														X				
propulsion	buried fuel lines			X				X											
	fuel inerting system												X		X	X			
	~29,000-pound engine thrust class		X				X												
	thrust-to-weight ratio >1		X				X												
flight control	fly-by-wire system for enhanced responsiveness						X												
	negative static stability for enhanced maneuverability						X												
	electronic-hydraulic stability augmentation system													X					
	fault tolerant control surfaces (aerodynamic redundancy)								X	X				X				X	
	ground collision avoidance w/dissimilar-source validation						X				X			X					
	override feature of computer's alpha-limiter														X				
	redundant electrical generating and distribution equipment								X										
	four sealed-cell batteries for fly-by-wire system								X										
	two separate and independent hydraulic systems								X			X	X						
armament	M61 20-mm six-barrel rotary cannon	X			X	X													
	AIM-9 infrared, beyond-visual range air-to-air missiles	X		X	X	X													
	rocket pods	X			X	X													
	anti-ship missiles	X			X	X													
	AGM-88 anti-radiation missiles	X			X	X													
	standoff precision strike weapons	X		X	X	X													
	AN/APG-68 pulse doppler radar																		X
	AN/ALQ-131 electronic countermeasures pod			X															
	AN/ALE-40 chaff and flare dispenser			X															
	fiber optic towed decoy			X															

In contrast to the first two empirical tests (*i.e.*, UH-60A and A-10A), no F-16 survivability features were left untraced to the design principle framework and no problems were identified with the design principle definitions. Interestingly, all seventeen design principles were utilized by at least one of the 36 identified F-16 survivability features.

Appendix C. Iridium Design Principles

Iridium is a space-based telecommunications system consisting of an interconnected network of 66 satellites (and six spares) distributed in six planes in low Earth orbit (LEO), ground-based system control facilities, gateways to the public switched telephone network, handheld phones, and communications links among nodes (Garrison, Pizzicaroli and Swan 1997). Iridium employs a unique concept-of-operations for commercial space communications by providing connectivity between satellites using dynamic crosslinks (Wertz and Larson 1999). While its economic failure is worthy of a value-centric analysis (de Weck, de Neufville and Chaize 2004), Iridium is also an interesting case application for the design principle framework in terms of survivability because the communications service is achieved not only by the individual Iridium satellites but also by the overall network architecture. Figure 9-3 provides an illustration of the major components an Iridium satellite.

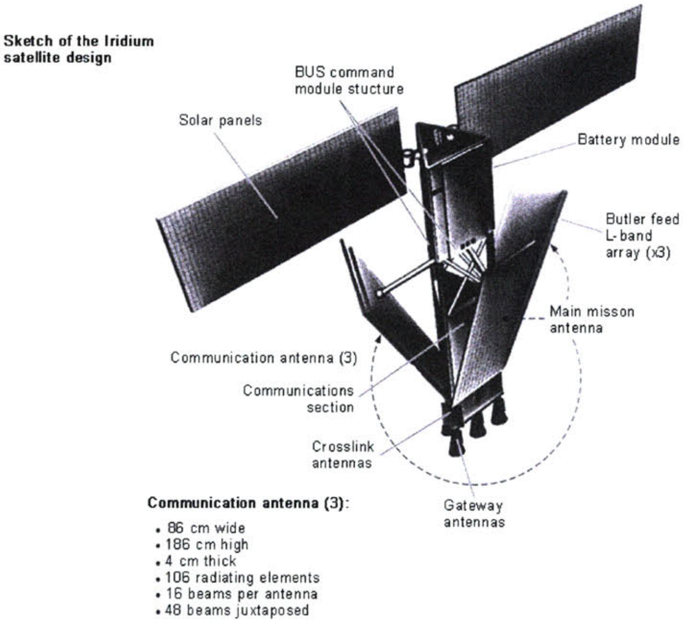


Figure 9-3. Iridium Satellite (Iridium LLC)

Iridium's constellation survivability has been evaluated by comparing packet rejection rates, hop counts, and average end-to-end delay performance of degraded Iridium constellations (Stenger 1996). These evaluations and related analyses (Fossa et al. 1998) have concluded that the Iridium communications service is robust to node removal. For example, even with 36 of the 66 spacecraft removed, the system is still functional (*i.e.*, packet delays do not exceed 178 milliseconds, well within an emergency value threshold of 400 milliseconds). Iridium's approach to survivability was validated to dramatic effect following the collision between an operational Iridium satellite and an old Russian military communications satellite on February 10, 2009. The hypervelocity, broadside collision occurred at an altitude of 790 km and shattered the 689 kg Iridium satellite into a debris cloud spreading out over a heavily used region of Low Earth Orbit (Morring, Butler and Mecham 2009). However, the collision resulted in only limited disruptions of service, with the company implementing a network solution within days (Iannotta 2009).

To test the baseline set of design principles, survivability features were gathered on the Iridium architecture from the literature (Comparetto and Hulkower 1994; Maine, Devieux and Swan 1995; Stenger 1996; Garrison, Pizzicaroli and Swan 1997; Pizzicaroli 1997; Swan 1997; Fossa, Raines et al. 1998; Karpiscak 1998; Lemme, Glenister and Miller 1998; Pratt et al. 1999; Puderbaugh et al. 2002; Iovanov et al. 2003; Swinerd et al. 2003; de Weck, de Neufville and Chaize 2004; He and Zhao 2007). In tracing Iridium design features to the design principles, the unit of analysis is the overall communications network. Design features include any aspect of the communications architecture (*e.g.*, satellite design, constellation configuration) that contributes to the survivability of the network, given the removal of constituent nodes or supporting infrastructural elements.

Upon identifying 33 survivability features of the Iridium architecture, the features were arranged into five categories (*i.e.*, satellite design, constellation configuration, communications links, ground segment, and deployment infrastructure), then traced to the seventeen general design principles and ODA loop. Table 9-3 presents the results of this empirical mapping.

Table 9-3. Tracing Iridium Survivability Features to Design Principles

		Design Principles																	
		Type I (Reduce Susceptibility)						Type II (Reduce Vulnerability)									Type III		
	Iridium: Sample Survivability Features	prevention	mobility	concealment	deterrence	preemption	avoidance	hardness	redundancy	margin	heterogeneity	distribution	reduction	fail-safe	evolution	containment	replacement	repair	ODA - exclusive
satellite	spare Motorola/Freescale PowerPC 603E processor								X										
	small exposed cross-sectional area (7 m²) to debris			X															
	end-of-life deorbit															X	X		
	functional independence of TT&C from payload												X			X			
	electronic equipment redundancy												X						
	ascent/deboost backup capability via ACS						X		X		X								
	60% hydrazine reserve (assuming 8-year life)						X			X									
	multi-point system health status monitoring																		X
	authenticated command messages							X											
	autonomous safing mode													X		X		X	
constellation	dynamic control of routing and channel selection										X			X	X		X		
	6 planes of 11 satellites separated by 31 6°											X							
	spare satellite in each orbital plane								X										
	altitude (780 km) above residual atmosphere						X												
	altitude (780 km) below Van Allen radiation belts						X												
	2150 active beams over the globe								X	X		X							
link	autonomous intersatellite links			X									X						
	availability of numerous alternate transmission paths		X				X		X			X					X		
	two gimbaled inter-plane crosslink antennas														X		X		
	omnidirectional secondary link for backup TT&C								X					X					
	guardband of 2 kHz between channels									X		X							
	rate 3/4 forward error correction coding							X										X	
	16 dB link margin									X									
	low altitude reduces exposure to a ground jammer			X															
ground	multiple physical gateways around the world								X			X							
	only single gateway required for global coverage									X			X	X					
	Backup Control Facility (BCF) in Rome, Italy								X			X							
	spaceborne handset to handset routing (autonomous)												X						
deployment	Delta II, Proton-K, and Long March 2C compatibility										X								
	launch risk distributed over 14 launches											X	X			X			
	launch sites in U S , China, and Kazakhstan										X	X							
	rapid assembly and test																X		
	interchangeable parts								X								X		

In contrast to the F-16 (Appendix B), the density of Type II mappings is higher than Type I mappings. Rather than emphasizing maneuverability away from threats or pursuing their active elimination, Iridium embraces a survivability strategy of graceful degradation and rapid reconstitution. While utilizing some legacy satellite survivability techniques to assure capability at the spacecraft level (*e.g.*, autonomous safe mode, redundant electronics, fuel reserves), the primary survivability of Iridium is achieved at the constellation level. (In fact, Iridium's reliability requirement for determining redundancy of critical spacecraft ·components is only a 0.58 probability of success for a five-year mission.) These constellation level survivability features include dynamic control and routing of satellite crosslinks around unavailable nodes, on-orbit satellite spares, and the ability to control all 66 operational spacecraft from a single ground facility. For example, following the shattering of the satellite on February 10, 2009, Iridium was able to move one of its in-orbit spares into the network constellation within a month (Iannotta 2009). "...[T]he design philosophy provides redundancy at the system level instead of the hardware configuration level. Autonomous operation and dynamic resource management and routing provide constellation failure mitigation. In effect, the traditional hardware redundancy is spread over many spacecraft" (Garrison, Pizzicaroli and Swan 1997).

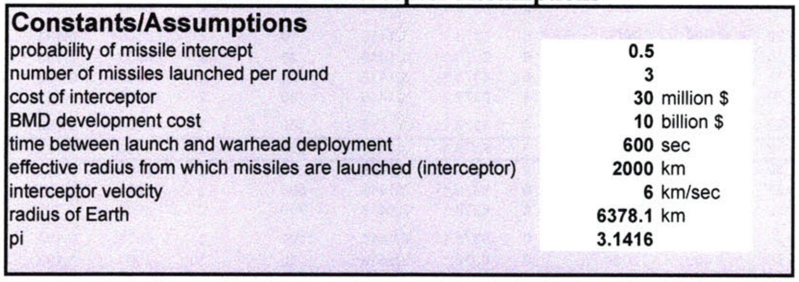
As with the F-16, no Iridium survivability features were left untraced to the design principle framework and no problems were identified with the design principle definitions. Fourteen of the seventeen design principles were utilized. (*Prevention*, *deterrence*, and *preemption* were not employed in this commercial communications architecture.)

Appendix D. Space-Based BMD Experiment

This appendix documents the assumptions, governing equations, and parametric analysis of the space-based BMD experiment. Given that the purpose of the computer experiment is to examine the use of cost-estimating relationships as one approach for front-end survivability analysis (rather than prescribe space-based BMD systems), a very simple model was utilized.

Table 9-4 documents the assumptions made in an engagement scenario. The first four assumptions are first-order estimates while the subsequent three assumptions are taken from the literature (Canavan and Teller 1990).

Table 9-4. Interceptor Assumptions



Constants/Assumptions		
probability of missile intercept	0.5	
number of missiles launched per round	3	
cost of interceptor	30	million $
BMD development cost	10	billion $
time between launch and warhead deployment	600	sec
effective radius from which missiles are launched (interceptor)	2000	km
interceptor velocity	6	km/sec
radius of Earth	6378.1	km
pi	3.1416	

The equations governing the model in the baseline case are given below. The first two equations are based on Canavan and Teller (1990), the third equation reflects the assumed decision logic of the BMD system, the fourth is a binomial probability of success (assuming interceptor independence), and the fifth equation is based on the non-recurring (development) cost and recurring cost assumptions.

$$range_{\text{int}} = radius_{effective} + velocity_{\text{int}} \cdot time_{deploy} \tag{9-1}$$

$$absentee = \frac{\pi \cdot (range_{\text{int}})^2}{4 \cdot \pi \cdot (radius_{earth})^2} \tag{9-2}$$

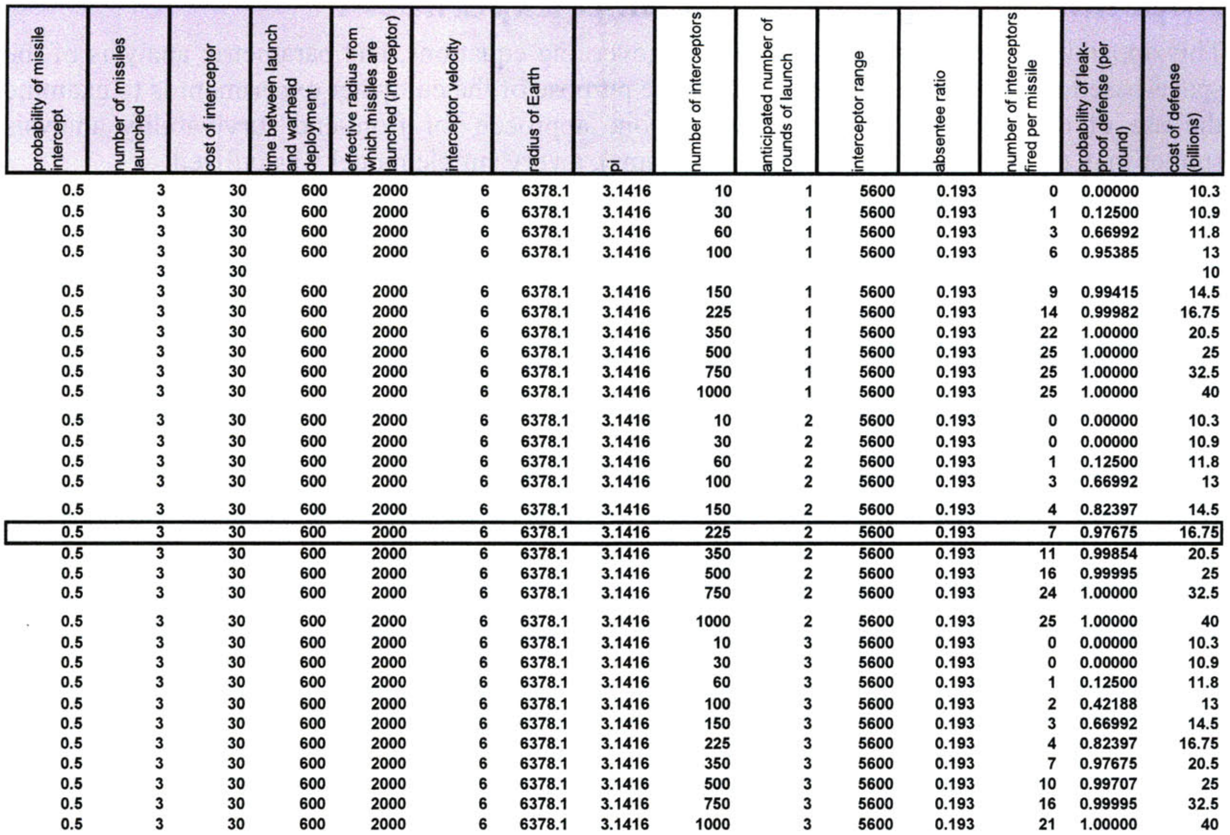
Number of interceptors fired per missile =
=Minimum[Integer(NumIntercept*absentee/MissilesLaunch/rounds), 25] (9-3)

Probability of leak proof defense = (1-(1-PInterMissile)^AllocatedInt)^MissilesLaunch) (9-4)

Cost of defense = CInter*NumIntercept/1000+Cdevelop (9-5)

Table 9-5 illustrates the results of the first-order space-based BMD model. As observed across the 30 candidate architectures, the costs of the systems vary from 10 to 40 billion dollars. The performance of each BMD—assessed as the probability of a leak-proof defense against a three-missile salvo (per round) from any point on the Earth's surface—ranges from less than 10% to performance in excess of five 9's of probability.

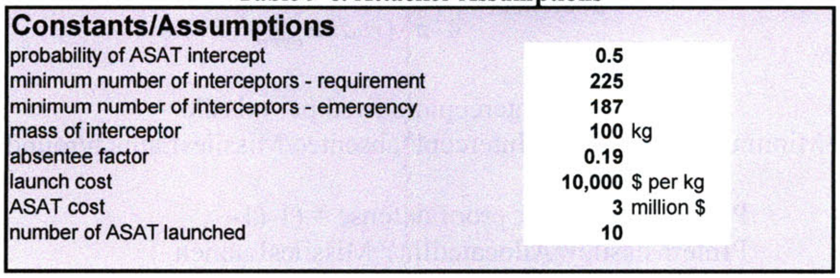
Table 9-5. Cost and Performance of Candidate Architectures (with Promising Baseline Outlined)



probability of missile intercept	number of missiles launched	cost of interceptor	time between launch and warhead deployment	effective radius from which missiles are launched (interceptor)	interceptor velocity	radius of Earth	pi	number of interceptors	anticipated number of rounds of launch	interceptor range	absentee ratio	number of interceptors fired per missile	probability of leak-proof defense (per round)	cost of defense (billions)
0.5	3	30	600	2000	6	6378.1	3.1416	10	1	5600	0.193	0	0.00000	10.3
0.5	3	30	600	2000	6	6378.1	3.1416	30	1	5600	0.193	1	0.12500	10.9
0.5	3	30	600	2000	6	6378.1	3.1416	60	1	5600	0.193	3	0.66992	11.8
0.5	3	30	600	2000	6	6378.1	3.1416	100	1	5600	0.193	6	0.95385	13
	3	30												10
0.5	3	30	600	2000	6	6378.1	3.1416	150	1	5600	0.193	9	0.99415	14.5
0.5	3	30	600	2000	6	6378.1	3.1416	225	1	5600	0.193	14	0.99982	16.75
0.5	3	30	600	2000	6	6378.1	3.1416	350	1	5600	0.193	22	1.00000	20.5
0.5	3	30	600	2000	6	6378.1	3.1416	500	1	5600	0.193	25	1.00000	25
0.5	3	30	600	2000	6	6378.1	3.1416	750	1	5600	0.193	25	1.00000	32.5
0.5	3	30	600	2000	6	6378.1	3.1416	1000	1	5600	0.193	25	1.00000	40
0.5	3	30	600	2000	6	6378.1	3.1416	10	2	5600	0.193	0	0.00000	10.3
0.5	3	30	600	2000	6	6378.1	3.1416	30	2	5600	0.193	0	0.00000	10.9
0.5	3	30	600	2000	6	6378.1	3.1416	60	2	5600	0.193	1	0.12500	11.8
0.5	3	30	600	2000	6	6378.1	3.1416	100	2	5600	0.193	3	0.66992	13
0.5	3	30	600	2000	6	6378.1	3.1416	150	2	5600	0.193	4	0.82397	14.5
0.5	3	30	600	2000	6	6378.1	3.1416	225	2	5600	0.193	7	0.97675	16.75
0.5	3	30	600	2000	6	6378.1	3.1416	350	2	5600	0.193	11	0.99854	20.5
0.5	3	30	600	2000	6	6378.1	3.1416	500	2	5600	0.193	16	0.99995	25
0.5	3	30	600	2000	6	6378.1	3.1416	750	2	5600	0.193	24	1.00000	32.5
0.5	3	30	600	2000	6	6378.1	3.1416	1000	2	5600	0.193	25	1.00000	40
0.5	3	30	600	2000	6	6378.1	3.1416	10	3	5600	0.193	0	0.00000	10.3
0.5	3	30	600	2000	6	6378.1	3.1416	30	3	5600	0.193	0	0.00000	10.9
0.5	3	30	600	2000	6	6378.1	3.1416	60	3	5600	0.193	1	0.12500	11.8
0.5	3	30	600	2000	6	6378.1	3.1416	100	3	5600	0.193	2	0.42188	13
0.5	3	30	600	2000	6	6378.1	3.1416	150	3	5600	0.193	3	0.66992	14.5
0.5	3	30	600	2000	6	6378.1	3.1416	225	3	5600	0.193	4	0.82397	16.75
0.5	3	30	600	2000	6	6378.1	3.1416	350	3	5600	0.193	7	0.97675	20.5
0.5	3	30	600	2000	6	6378.1	3.1416	500	3	5600	0.193	10	0.99707	25
0.5	3	30	600	2000	6	6378.1	3.1416	750	3	5600	0.193	16	0.99995	32.5
0.5	3	30	600	2000	6	6378.1	3.1416	1000	3	5600	0.193	21	1.00000	40

Following establishment of a baseline space-based BMD system, the computer experimented focused on calculating the outcome of a given attack and the resources expended by the attacker and defender. Table 9-6 lists the assumptions made regarding the attacker effectiveness and cost.

Table 9-6. Attacker Assumptions



Constants/Assumptions		
probability of ASAT intercept	0.5	
minimum number of interceptors - requirement	225	
minimum number of interceptors - emergency	187	
mass of interceptor	100	kg
absentee factor	0.19	
launch cost	10,000	$ per kg
ASAT cost	3	million $
number of ASAT launched	10	

Table 9-7. Candidate Distributed and Concentrated BMD Architectures

probability of ASAT intercept	minimum number of interceptors - requirement	minimum number of interceptors - emergency	mass of interceptor	absentee factor	launch cost	ASAT cost	number of ASAT launched	number of carrier vehicles	number of interceptors per carrier vehicle	total number of interceptors	mass of carrier vehicle	required number of interceptors - field of regard	emergency number of interceptors - field of regard	expected number of interceptors - field of regard	cost of attack	cost of defense	meet expected value threshold (i.e., requirement)?	meet emergency value threshold (i.e., survivable)?	cost-exchange ratio (defense/attack)	survivability
0.5	225	187	100	0.19	10,000	3	10	200	1	200	100.0	42	35	33	30	26	no	no	0.87	0.00
0.5	225	187	100	0.19	10,000	3	10	210	1	210	100.0	42	35	34.9	30	46	no	no	1.53	0.00
0.5	225	187	100	0.19	10,000	3	10	220	1	220	100.0	42	35	36.8	30	66	no	yes	2.20	0.26
0.5	225	187	100	0.19	10,000	3	10	230	1	230	100.0	42	35	38.7	30	86	no	yes	2.87	0.53
0.5	225	187	100	0.19	10,000	3	10	235	1	235	100.0	42	35	39.65	30	96	no	yes	3.20	0.66
0.5	225	187	100	0.19	10,000	3	10	240	1	240	100.0	42	35	40.6	30	106	no	yes	3.53	0.80
0.5	225	187	100	0.19	10,000	3	10	245	1	245	100.0	42	35	41.55	30	116	no	yes	3.87	0.94
0.5	225	187	100	0.19	10,000	3	10	250	1	250	100.0	42	35	42.5	30	126	yes	yes	4.20	1.00
0.5	225	187	100	0.19	10,000	3	10	260	1	260	100.0	42	35	44.4	30	146	yes	yes	4.87	1.00
0.5	225	187	100	0.19	10,000	3	10	270	1	270	100.0	42	35	46.3	30	166	yes	yes	5.53	1.00
0.5	225	187	100	0.19	10,000	3	10	280	1	280	100.0	42	35	48.2	30	186	yes	yes	6.20	1.00
0.5	225	187	100	0.19	10,000	3	10	290	1	290	100.0	42	35	50.1	30	206	yes	yes	6.87	1.00
0.5	225	187	100	0.19	10,000	3	10	100	2	200	158.7	42	35	28	30	23	no	no	0.78	0.00
0.5	225	187	100	0.19	10,000	3	10	105	2	210	158.7	42	35	29.9	30	41	no	no	1.38	0.00
0.5	225	187	100	0.19	10,000	3	10	110	2	220	158.7	42	35	31.8	30	59	no	no	1.97	0.00
0.5	225	187	100	0.19	10,000	3	10	115	2	230	158.7	42	35	33.7	30	77	no	no	2.57	0.00
0.5	225	187	100	0.19	10,000	3	10	120	2	240	158.7	42	35	35.6	30	95	no	yes	3.17	0.09
0.5	225	187	100	0.19	10,000	3	10	125	2	250	158.7	42	35	37.5	30	113	no	yes	3.77	0.36
0.5	225	187	100	0.19	10,000	3	10	130	2	260	158.7	42	35	39.4	30	131	no	yes	4.36	0.63
0.5	225	187	100	0.19	10,000	3	10	135	2	270	158.7	42	35	41.3	30	149	no	yes	4.96	0.90
0.5	225	187	100	0.19	10,000	3	10	140	2	280	158.7	42	35	43.2	30	167	yes	yes	5.56	1.00
0.5	225	187	100	0.19	10,000	3	10	145	2	290	158.7	42	35	45.1	30	185	yes	yes	6.16	1.00
0.5	225	187	100	0.19	10,000	3	10	70	3	210	208.0	42	35	24.9	30	39	no	no	1.30	0.00
0.5	225	187	100	0.19	10,000	3	10	75	3	225	208.0	42	35	27.75	30	64	no	no	2.14	0.00
0.5	225	187	100	0.19	10,000	3	10	80	3	240	208.0	42	35	30.6	30	90	no	no	2.99	0.00
0.5	225	187	100	0.19	10,000	3	10	85	3	255	208.0	42	35	33.45	30	115	no	no	3.84	0.00
0.5	225	187	100	0.19	10,000	3	10	90	3	270	208.0	42	35	36.3	30	141	no	yes	4.68	0.19
0.5	225	187	100	0.19	10,000	3	10	92	3	276	208.0	42	35	37.44	30	151	no	yes	5.02	0.35
0.5	225	187	100	0.19	10,000	3	10	95	3	285	208.0	42	35	39.15	30	166	no	yes	5.53	0.59
0.5	225	187	100	0.19	10,000	3	10	97	3	291	208.0	42	35	40.29	30	176	no	yes	5.87	0.76
0.5	225	187	100	0.19	10,000	3	10	100	3	300	208.0	42	35	42	30	191	no	yes	6.38	1.00
0.5	225	187	100	0.19	10,000	3	10	105	3	315	208.0	42	35	44.85	30	217	yes	yes	7.23	1.00
0.5	225	187	100	0.19	10,000	3	10	110	3	330	208.0	42	35	47.7	30	242	yes	yes	8.07	1.00
0.5	225	187	100	0.19	10,000	3	10	115	3	345	208.0	42	35	50.55	30	268	yes	yes	8.92	1.00
0.5	225	187	100	0.19	10,000	3	10	50	4	200	252.0	42	35	18	30	21	no	no	0.71	0.00
0.5	225	187	100	0.19	10,000	3	10	55	4	220	252.0	42	35	21.8	30	54	no	no	1.79	0.00
0.5	225	187	100	0.19	10,000	3	10	60	4	240	252.0	42	35	25.6	30	86	no	no	2.88	0.00
0.5	225	187	100	0.19	10,000	3	10	65	4	260	252.0	42	35	29.4	30	119	no	no	3.97	0.00
0.5	225	187	100	0.19	10,000	3	10	70	4	280	252.0	42	35	33.2	30	152	no	no	5.05	0.00
0.5	225	187	100	0.19	10,000	3	10	75	4	300	252.0	42	35	37	30	184	no	yes	6.14	0.29
0.5	225	187	100	0.19	10,000	3	10	77	4	308	252.0	42	35	38.52	30	197	no	yes	6.57	0.50
0.5	225	187	100	0.19	10,000	3	10	80	4	320	252.0	42	35	40.8	30	217	no	yes	7.23	0.83
0.5	225	187	100	0.19	10,000	3	10	85	4	340	252.0	42	35	44.6	30	249	yes	yes	8.31	1.00
0.5	225	187	100	0.19	10,000	3	10	90	4	360	252.0	42	35	48.4	30	282	yes	yes	9.40	1.00
0.5	225	187	100	0.19	10,000	3	10	95	4	380	252.0	42	35	52.2	30	315	yes	yes	10.49	1.00

Table 9-7 illustrates all 45 architectures considered, their performance, and their cost relative to the attacker. Section 5.1.3 describes the governing equations. In varying the number of interceptors per carrier vehicle from n=1 to n=4, the architecture that exceeds both the emergency and expected value thresholds with *the lowest cost-exchange ratio* is the Brilliant Pebbles singlet case of n=1 when 250 interceptors are deployed.

Appendix E. MATE for Survivability Activity Descriptions

This appendix provides an extended description of each of the 29 tasks comprising MATE for Survivability. Following the "cookbook" template of describing the MATE process in Ross (2003), each task is discussed in five parts: (1) inputs, (2) outputs, (3) task description, (4) task dependencies, and (5) worked example. Rather than continuously referring the reader back to Chapter 6, the abbreviated task descriptions from the chapter are included in the detailed task descriptions.

Phase 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 utility function, (1.4) specify emergency value threshold(s), and (1.5) specify permitted recovery time(s).

Task 1.1 Develop Mission Statement

Inputs:

Although the first task in the design process, developing the mission statement is coupled with the second task of identifying a decision-maker for the system development. Writing a mission statement requires the analyst to be in communication with the system decision-maker.

Outputs:

The outputs of Task 1.1 are a concise statement of stakeholder needs, the rationale for those needs, and the expected scope of the system analysis.

Description:

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.

Dependencies:

Inputs: 1.2
Outputs: 1.2, 1.3, 1.4, 1.5, 3.1

Space Tug Example:

The purpose of the study is to analyze system alternatives for a national capability for the timely repair and/or relocation of satellites in a low-Earth orbit. The general system concept is to deploy an orbital transfer vehicle that can rendezvous and dock with space objects and perform any desired stabilization or relocation maneuvers. The vehicle should maximize cost-effectiveness and be survivable to an environment characterized by a high flux of debris.

Task 1.2 Identify Decision-maker

Inputs:

The need and context of the need helps clarify where the critical system stakeholders are located.

Outputs:

The key output of Task 1.2 is the identification of an actual or proxy decision-maker (*i.e.*, stakeholder with influence over the allocation of resources for a project) with a rigorous understanding of the value proposition for developing a system and of the system's use context. The decision-maker's understanding should include knowledge of performance requirements and of financial constraints.

Description:

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. 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.[59] 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.

Dependencies:

Inputs: 1.1
Outputs: 1.1, 1.3, 1.4, 1.5, 2.1

Space Tug Example:

For the space tug computer experiment, a proxy decision-maker was selected from the analyst team to represent a DARPA program manager interested in a general-purpose orbital transfer vehicle (*i.e.*, military and commercial applications).

Task 1.3 Elicit Multi-Attribute Utility Function

Inputs:

In order to quantitatively specify the evaluation criteria for the system analysis, it is necessary first to understand the mission context and to identify a decision-maker. Furthermore, iteration on the value function may occur based upon changing stakeholder needs and emergent lessons from the tradespace analysis (*e.g.*, lack of feasible designs given overly-stringent requirements).

Outputs:

The outputs of Task 1.3 are a set of attributes (*i.e.*, decision-maker-perceived metrics that measure how well decision-maker-defined objectives are met), the acceptability ranges associated with the attribute set, single-attribute utility functions, (defining user satisfaction ranging from 0, minimally acceptable, to 1, highest of expectations), and a multi-attribute utility function. The multi-attribute utility function provides a universal metric against which the performance of design alternatives operating in a nominal environment may be assessed.

[59] Ross (2006) demonstrates how the assumption of a unitary decision-maker may be relaxed within a MATE analysis for multi-stakeholder insights.

Description:

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.[60] 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 benefit is delivered for exceeding that level). In order to satisfy the axioms of Multi-Attribute Utility Theory (Keeney and Raiffa 1993), the analyst must ensure that the attribute set is defined by the decision-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 benefit 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 (von Neumann and Morgenstern 1953). For systems that have multiple attributes (N) with varying weights (k_i), computing a single scalar value function that fully reflects decision-maker preferences can be difficult. As a proxy for benefit, the multi-attribute utility function, $U(\underline{X})$, as defined in Keeney and Raiffa (1993), is used to reflect preference orderings.

$$\begin{aligned} &KU(\underline{X})+1=\prod_{i=1}^{N}[Kk_iU_i(X_i)+1] \quad \text{for} \quad K\neq 0 \\ \text{or} \quad &U(\underline{X})=\sum_{i=1}^{N}U(X_i)k_i \quad \text{for} \quad K=1 \end{aligned} \tag{9-6}$$

$$\text{where K is the solution to } K+1=\prod_{i=1}^{N}[Kk_i+1]; \text{ and } -1<K<1, K\neq 0. \tag{9-7}$$

The issue of stakeholder value elicitation is core to the MATE process and well-documented in existing literature. Ross (2003) 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 (2003) discusses the implications of simplifying the elicitation of single-attribute utility functions using hand-drawn utility curves and linear, risk-averse preference relationships.

Dependencies:

Inputs: 1.1, 1.2, 5.4
Outputs: 1.4, 1.5, 2.2, 2.3, 2.4, 5.1, 5.2, 5.4

Space Tug Example:

Three attributes comprise the space tug's multi-attribute utility function: total ΔV capability, capability of the grappling system, and response time. As illustrated in Figure 9-4, the single

[60] Attributes must be complete, operational, decomposable, non-redundant, minimal, and perceived independent (Keeney and Raiffa 1993).

attribute utility function for ΔV is continuous while discrete steps characterize the utility delivered by the grappling system. Response time utility is a binary distribution where all non-electric propulsion vehicles deliver utility 1 and electric propulsion receives a minimally-acceptable score of 0. When attribute levels are worse than minimally-acceptable levels, the utility function is undefined and any designing delivering that attribute level is removed from the tradespace. For example, the utility of any space tug with a capability level below "low" during normal operating conditions is undefined. (Conversely, performance in an attribute better than the level associated with a utility of 1 cannot gain utility above this maximum level).

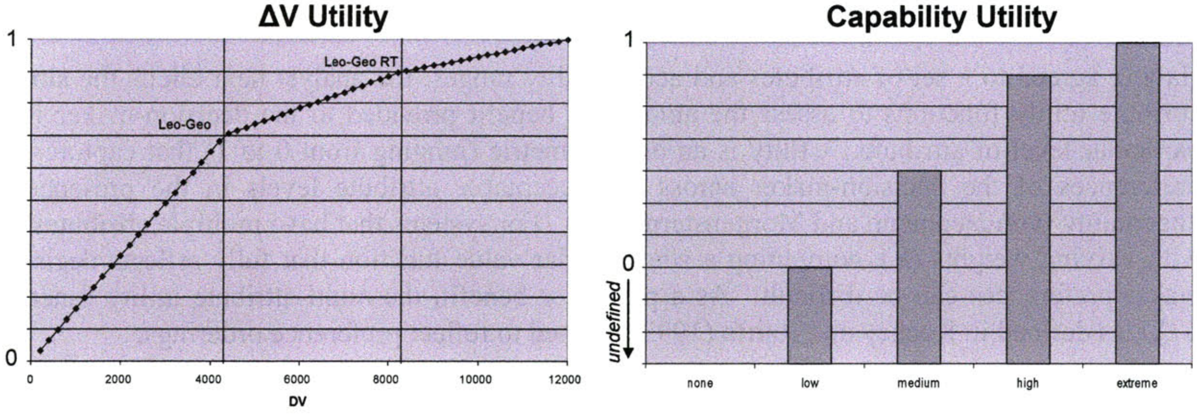


Figure 9-4. Single-Attribute Utility Functions for Space Tug during Nominal Conditions

A linear weighted sum is used for multi-attribute utility with weights assigned of 0.6 for ΔV, 0.3 for grappling capability, and 0.1 for response time.

Task 1.4 Specify Emergency Value Threshold

Inputs:

In order to specify the minimum acceptable level of value to be delivered during and immediately after a disturbance (V_e in Figure 3-2), the analyst consults with the identified decision-maker to probe whether lower performance across the attributes may be temporarily acceptable.

Outputs:

The output of Task 1.4 is a set of worst-case attribute levels for the set of single-attribute utility functions during, and in the aftermath, of a disturbance event. Depending on decision-maker preferences, these levels may either be constant or vary across nominal and disturbed environmental states.

Description:

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 (Bayer 2007).

As discussed in Section 3.3.4, 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 epochs. A general response to this implication is to elicit applicable multi-attribute utility functions across all potential epochs 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 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 and recovery epochs 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.

Dependencies:
Inputs: 1.1, 1.2, 1.3
Outputs: 1.5, 6.4, 7.1

Space Tug Example:
In following the discussion in Section 3.3.4, the attribute set comprising the multi-attribute utility function is constant across normal, disturbance, and recovery epochs for space tug. However, the acceptability range of the utility function for grappling capability is relaxed during the disturbance and recovery epochs to include "none" as a temporarily acceptable level. Therefore, a utility of 0 (in the capability utility plot in Figure 9-4) is now achieved at the bottom of the previously undefined range. In addition, the shape of the single-attribute utility curve is reassessed across the expanded acceptability range. Single-attribute utility curves for total ΔV capability and response time as well as the linear aggregation for the multi-attribute utility function are unmodified.

Task 1.5 Specify Permitted Recovery Time

Inputs:
The analyst consults with the decision-maker to identify the maximum acceptable duration for the system to meet only the emergency value threshold (in lieu of meeting the required value threshold).

Outputs:
The output of Task 1.5 is the permitted recovery time following the beginning of a disturbance (T_r in Figure 3-2).

Description:
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.

Dependencies:
Inputs: 1.1, 1.2, 1.3, 1.4, 4.5
Outputs: 6.4, 7.1

Space Tug Example:
Given that the space tug is envisioned as an infrastructure capability for performing infrequent servicing operations, the permitted recovery time following a debris event is one year.

Phase 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

Inputs:
Having developed the mission statement and identified a decision-maker, any constraints on the design effort should be elicited from critical system stakeholders (*e.g.*, customer, builder, user). Feedback from the subsequent tradespace analysis may cause the decision-maker to modify the constraints imposed on the design effort.

Outputs:
The outputs of Task 2.1 may include formal guidance regarding preferred system concepts, available technologies, and available supporting infrastructures.

Description:
Constraints are requirements that must be satisfied in order for the system 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 (2006), some constraints are subject to change and must be carefully tracked as shifts may significantly alter the "best" outcome for a particular problem.

Dependencies:
Inputs: 1.1, 1.2, 2.2, 8.1
Outputs: 2.2, 5.2, 5.3

Space Tug Example:
The only explicit constraints in the space tug computer experiment are physical constants. However, current satellite bus technology is implicitly assumed by basing design constants on empirical data (*e.g.*, specific impulse of engines).

Task 2.2 Propose Design Variables

Inputs:

In order to determine what concepts to parameterize for tradespace analysis, the designer inspects the decision-maker attributes and uses expert judgment to propose candidate design variables. Context for this process is provided by the mission statement, and limits for the proposed system concepts are provided by the identified constraints. Feedback from the subsequent tradespace analysis may cause the designer to modify the design variables under consideration.

Outputs:

The output of Task 2.2 is a list of proposed design variables that will be traced to the attributes and allow preliminary development of the model.

Description:

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.

Dependencies:

Inputs: 1.1, 1.3, 2.1, 8.1
Outputs: 2.1, 2.3, 5.1

Space Tug Example:

The space tug design variables are propulsion system, fuel load, and equipment mass.

Task 2.3 Map Design Variables to Attributes

Inputs:

The inputs to Task 2.3 are a set of proposed design variables and a finalized list of attributes.

Outputs:

The output of Task 2.3 is an estimation of the impact of each design variable on each attribute to aid in the finalization of the baseline design vector and in the development of the performance model.

Description:

Design variables are mapped to the attributes to ensure that the system concepts address the needs articulated by the decision-maker. 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.)

Four general steps comprise mapping the design variables to attributes. First, a matrix is drawn with the elicited attributes as columns and the proposed design variables as rows (or vice versa). 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 rows are summed to provide an estimate of the importance of a particular design variable. (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.) Fourth, the columns 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.

Dependencies:
Inputs: 1.3, 2.2, 5.2
Outputs: 2.4, 5.1, 5.2

Space Tug Example:
Table 6-1 shows the mapping between the design variables and attributes of space tug.

Task 2.4 Finalize Baseline Design Vector

Inputs:
To finalize the baseline design vector, the analyst consults the final set of attributes, proposed set of design variables, and the estimated impact relationships. The baseline design vector may be modified based on feedback from development of the system model.

Outputs:
The output of Task 2.4 is the finalized set of baseline design variables and associated enumeration and sampling strategies.

Description:
The concept generation phase is completed with the finalization of the design variables, including the range and step size for each design variable. 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.

Dependencies:
Inputs: 1.3, 2.2, 2.3, 5.2
Outputs: 3.1, 3.3, 4.1, 4.2, 4.5, 5.1

Space Tug Example:
Table 6-2 shows the baseline design vector for space tug.

Phase 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

Inputs:
Enumerating disturbance types requires familiarity with the operational environment and knowledge of the candidate system concepts.

Outputs:
The output of Task 3.1 is a list of disturbance types to focus the data collection effort on disturbance magnitude and occurrence.

Description:
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).

Dependencies:
Inputs: 1.1, 2.4
Outputs: 3.2, 4.1

Space Tug Example:
Spacecraft operating in a low-inclination orbit at 800 km may require design changes to cope with trapped radiation, micrometeorites, and debris (Pisacane 2008).

Task 3.2 Gather Data on Disturbance Magnitude and Occurrence

Inputs:
The input to Task 3.2 is a list of disturbance types for the system concept(s) under consideration.

Outputs:
The output of Task 3.2 is an importance score for each disturbance type based on the magnitude of impact and likelihood of occurrence.

Description:
Task 3.2 is to gather data on the magnitude and occurrence of different disturbance types to support subsequent model development. 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

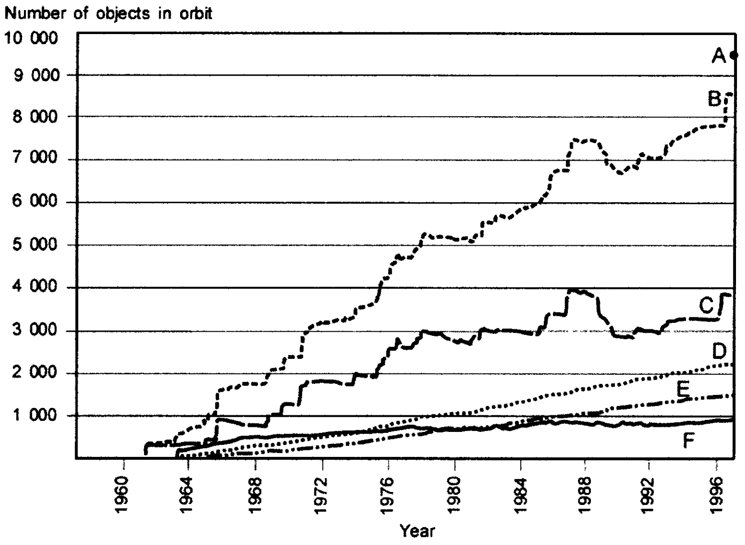
disturbances are not of equal concern, an importance score for each disturbance is assigned based on the magnitude of impact and likelihood of occurrence.

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.

Dependencies:
Inputs: 3.1
Outputs: 3.3, 4.2, 4.3, 4.5

Space Tug Example:
Pisacane (2008) provides a relative ranking of space environment disturbances on mission impact (with a scale of 1-10). In low-inclination LEO, micrometeorites receive a 3 (may require design changes), trapped radiation receives a 5 (may reduce mission effectiveness), and debris receives a 7 (may shorten mission). Given the relative importance of debris and limited scope of the space tug computer experiment, debris is the only disturbance for which empirical data is gathered.

There are millions of kilograms of objects in Earth orbit that pose a series of challenges to space mission designers. Normal satellite operations frequently deposit orbital debris (*e.g.*, dead satellites, spent upper stages, separation devices, bolts, and paint chips). Using a distributed network of radar and optical sites that are operated by the U.S. Air Force, Army and Navy, U.S. Space Command tracks more than 9,000 space objects with major axes in excess of ten centimeters. An additional 100,000 objects ranging from one to ten centimeters is estimated to be in Earth orbit and it is estimated that the debris population continues to grow by more than 175 metric tons per year (Futron 2002).



A Total number of objects, including objects not contained in the official catalogue
B: Total number of objects, based on the official catalogue
C: Fragmentation debris; fragments are counted since the year of event; fragmentation parents are counted as intacts until the date of event, since the event date the parents are counted as fragments
D Spacecraft
E: Rocket bodies
F: Operational debris, operational debris related to a launch are counted since the year of launch, Salyut 4, 5, 6, 7 and Mir operational debris are not counted since the date of launch of the parent but since a more realistic date

Figure 9-5. Number of Space Objects in US Catalog (UN 1999)

The population of tracked objects presents a manageable debris hazard, even to large spacecraft such as the International Space Station. However, including untrackable objects into a debris hazard assessment increases the flux rate by orders of magnitude. While 1 mm objects will likely only cause surface degradation, a 1 cm collision at high relative velocities is capable of producing significant impacts (Wertz and Larson 1999).

Determination of the precise distribution of near-Earth debris is a difficult proposition. Although the trackable population has grown linearly since 1960 (Figure 9-5), it is unclear how much the undetectable population has grown. This difficulty is compounded by the fact that the <10 cm diameter population is more strongly influenced by fragmentations. Predictions of the absolute number of debris objects and flux (*i.e.*, expected number of collisions per cross-sectional area per year) require accurate models of debris sources and sinks. These models are calibrated by both sampling portions of the spatial volume around Earth for debris density and observing impact rates on spacecraft surfaces returned to Earth (Wertz and Larson 1999). Inferences regarding the population of debris in models maintained by civil space agencies are continually updated as understanding of the environment grows.

In order to understand the threat environment for a given orbit, it is necessary to obtain a probability density distribution of orbital debris as a function of both mass and relative velocity (as momentum is the key determinant of damage). This distribution may be calculated by obtaining distributions of orbital debris flux and applying a distribution of relative velocity or by obtaining debris density and utilizing an average relative velocity.

To assess debris collision risk in LEO, the ORDEM2000 model maintained by NASA's Orbital Debris Program Office at Johnson Space center is applied to candidate space tug orbits. ORDEM2000 is a computer-based engineering model utilizing a maximum likelihood estimator to convert observations into debris population probability distribution functions (Liou et al. 2002). Several sources of debris samples inform the database:

- Space Surveillance Network (SSN) catalog
- Haystack and Haystack Auxiliary radar data
- Goldstone radar data
- Impact measurements from the Long-Duration Exposure Facility (LDEF)
- Hubble Space Telescope Solar Array impact data
- European Retrievable Carrier impact data
- Space Shuttle window and radiator impact data
- Space Flyer Unit data
- Mir impact data

The ORDEM2000 model is based on five debris populations which are distinguished based on size thresholds: 10μm and greater, 100 μm and greater, 1 cm and greater, 10 cm and greater, and 1 m and greater. The distribution of these five populations is highly nonlinear. Figure 9-6 shows how frequency of particles grows logarithmically at smaller sizes (*e.g.*, there are ~8,000 objects greater than 10 cm, ~11,000 between 1 and 10 cm, and ~35 million between .1 and 1 cm) (Remo 2005). The SSN catalog is used to build the 10 cm and 1 m populations, Haystack radar data is used to build the 1 cm population, and LDEF is used to build the 10μm and 100 μm populations. No systems are available for directly sampling the 1 mm population. Instead, ORDEM2000 linearly interpolates between the 100 μm and 1 cm populations (with Goldstone radar data of 3 mm objects used to justify the interpolation).

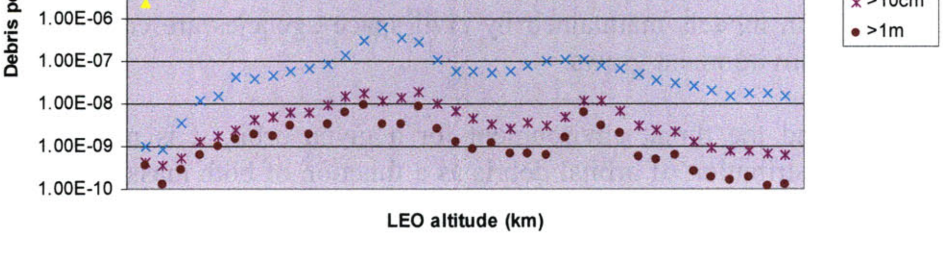


Figure 9-6. Spatial Density of LEO Orbital Debris

The ORDEM2000 model was run for candidate space tug altitudes ranging from 150-1950 km. Figure 6-2 shows the distribution of average orbital velocity for LEO debris. For a limited range of altitude, debris velocity appears constant across >1 cm populations which may simplify relative velocity calculations (*i.e.*, accounting for difference between debris and space tug velocity vectors) for the objects most likely to cause series space tug damage.

In order to understand the implications of the results obtained from the models of LEO debris, it is necessary to know their degree of precision (or lack thereof) by understanding the underlying physical relationships between the sampling observations and the inferences drawn about the debris population. One method used for calculating the surface area of orbital debris—correlating radar cross-section (RCS) observations with the effective area of space objects—is a good illustration of the need to recognize and account for sampling errors in the engineering models. Badhwar and Anz-Meador (1989) compared RCS measurements from the Eglin radar operating at 70 cm wavelength to 196 satellites of known shape, size, and mass. Knowledge of these 196 satellites was used to calibrate the calculated mass to the observed mass and to develop a relationship between the mean RCS and the effective area of the object.

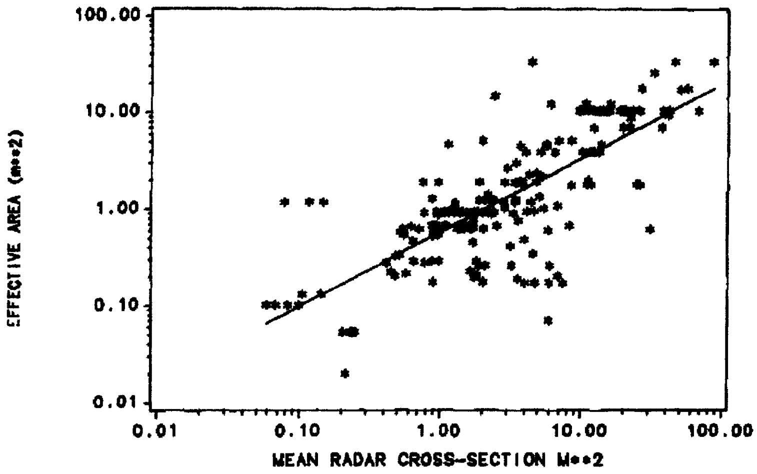


Figure 9-7. Correlating RCS to Area (Badhwar and Anz-Meador 1989)

Figure 9-7 is Badhwar and Anz-Meador's plot of the effective (projected surface) area versus the mean of the RCS for the objects with known geometry as well as the best-fit least-squares line to a power law fit. The proposed power law relation for effective area to RCS is A_eff=k[RCS]^.76. The proportion of variance accounted for is computed with an R-square calculation of .578, indicating only a moderately good fit (*e.g.*, the assumption that all objects were tumbling in random directions when observed by the Eglin radar is only an approximation of reality as these objects would be expected to become gravity gradient stabilized in a given orientation, presenting a non-random face to the radar beam).

To establish a power law relationship between mass and effective area, Badhwar and Anz-Meador (1989) applied a regression analysis to 2600 debris fragments. By dividing the RCS of the debris by the area-to-mass ratio (calculated using the orbital elements), a plot was generated of the calculated mass against the effective area (Figure 9-8).

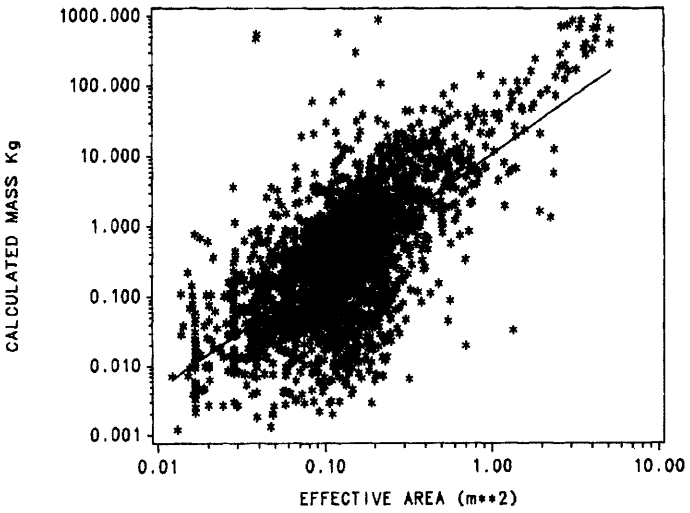


Figure 9-8. Correlating Area to Mass (Badhwar and Anz-Meador 1989)

Badhwar and Anz-Meador contend that this establishes a power law relation, m=kA^(1.86), for relating debris mean mass to mean effective area. However, there is no discussion of the proportion of variance accounted for nor a discussion of whether the data satisfies the assumptions required for inferences to be discussed. For example, Figure 9-8 clearly exhibits heteroscedastic data with a larger spread of calculated masses towards the lower-end of effective areas. Given that effective area is derived from the RCS, it is understandable that there would be more noise in the data for smaller pieces of orbital debris. However, the authors do not discuss why a linear regression was used despite a lack of homoscedastic data. The spread in values can be attributed to a variety of reasons, but only increased heterogeneity among smaller objects *(e.g.*, objects with larger masses are expected to be largely aluminum while smaller objects can be aluminum or less dense plastics or insulation materials) is discussed. To address the need for normally distributed data, a subsequent figure in Badhwar and Anz-Meador (1989) does a good job showing that the log of the mass is fairly Gaussian. Although valid for capturing first-order effects (and informing a first-order parametric study of space tug survivability), one should not characterize the validity of these relationships as precise. (The authors note in the conclusion that their overall technique is valid to only about 30%.)

Indeed, although engineering models of LEO orbital debris models make every effort possible for verification and validation (*e.g.*, NASA's ORDEM2000 has compared its model to precise radar observations and to in-situ measurements of Space Shuttle, Hubble, and Mir debris flux), it is important to remember that the results are not absolute and subject to sampling error.

Task 3.3 Develop System-Independent Models of Disturbance Environment

Inputs:

The input to Task 3.3 is a set of causal relationships, empirical data, and expert judgments that characterizes the types, magnitudes, and frequencies of disturbances in the operational environment of the envisioned system concept.

Outputs:
The output of Task 3.3 is a set of system-independent disturbance models with system-specific hooks.

Description:
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 for applications to all design vector variations within a given system concept.

Dependencies:
Inputs: 2.4, 3.2
Outputs: 5.1, 6.1, 6.2

Space Tug Example:
As discussed in Section 5.3.2, a general model of orbital debris was developed by calculating conjunction events around a volume encompassing all sizes of candidate space tug vehicles. The conjunctions are generated according to a Poisson process where the arrival rate is determined by the debris flux. All space tugs are assumed to launch in 2009 into an 800 km circular orbit at a 42.6° inclination. Flux is assumed isotropic and constant over the ten-year operational life.

The distribution of momentum for the impacting debris is computed by assuming an average collision velocity of 7 km/s (Figure 6-2) and a probability density function of debris mass. The distribution of mass is based on the spatial density of debris diameters (Figure 5-10) and relationships for relating debris diameter to debris area and debris area to debris mass (Badhwar and Anz-Meador 1989).

Phase 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 Design Principles

Inputs:
Generating survivable concepts requires knowledge of the baseline system concept and of the disturbances of concern. The subsequent tradespace analysis may feedback to Task 4.1 if the concepts initially enumerated fail to meet basic survivability requirements.

Outputs:
The output of Task 4.1 is a set of concept enhancements associated with each survivability principle.

Description:

The seventeen design principles (Section 4.4) 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).

Dependencies:

Inputs: 2.4, 3.1, 8.1
Outputs: 4.2

Space Tug Example:

Figure 6-3 shows the concept enhancements for space tug to orbital debris. The five concepts span the three types of survivability.

Task 4.2 Parameterize Survivable Concepts with Design Variables

Inputs:

The inputs to Task 4.2 are the baseline design vector, disturbance data, and set of survivable concepts.

Outputs:

The outputs of Task 4.2 are a set of design variables and associated enumeration ranges that collectively represent the survivability concepts.

Description:

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.

Dependencies:

Inputs: 2.4, 3.2, 4.1
Outputs: 4.3, 8.1

<u>*Space Tug Example*</u>:

The five survivability concepts for space tug are active collision avoidance, reduced exposed cross-sectional area, bumper shielding, increased capability margin, and on-orbit repair. Design variables for active collision avoidance include additional propellant, data-sharing with tracking facilities, and coordination with co-orbiting spacecraft operators (Wertz and Larson 1999). A design variable for bumper shielding may consist of dedicated mass or shielding thickness. On-orbit repair may be represented as servicing interface option (*e.g.*, none, tug, refuel, component change-out, and general repair). The remaining two survivability concepts—reduce exposed cross-sectional area and increase capability margin—are intermediate variables derived from the baseline design vector. In other words, the initial concept generation activity already incorporates these survivability considerations in the tradespace.

Task 4.3 Assess Ability of Design Variables to Mitigate Disturbances

<u>*Inputs*</u>:

The inputs to Task 4.3 are the survivability design variables and data on disturbance type, magnitude, and occurrence.

<u>*Outputs*</u>:

The output of Task 4.3 is an estimation of the impact of each survivability design variable on each disturbance to aid in the finalization of the design vector and in the development of the survivability model.

<u>*Description*</u>:

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 used.

<u>*Dependencies*</u>:

Inputs: 3.1, 3.2, 4.2
Outputs: 4.4, 5.1, 6.1, 6.2, 6.3

Space Tug Example:
For space tug, bumper shielding was estimated to have a high impact on mitigating orbital debris. On-orbit servicing for repair and active collision avoidance were estimated to have medium and low impacts, respectively.

Task 4.4 Filter Survivability Design Variables

Inputs:
The input to Task 4.4 is the assessment of the level of impact of the survivability design variables on the disturbances.

Outputs:
The output of Task 4.4 is an aggregate impact score for the consolidated design variables under consideration.

Description:
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.

Dependencies:
Inputs: 3.2, 4.3
Outputs: 4.5

Space Tug Example:
Given the small number of survivability design variables in the space tug computer experiment and single focus on the threat posed by orbital debris, the analysis did not require building a survivability design matrix to filter the design vector. (Section 7.2.4 provides an example of the survivability design matrix in the satellite radar case application.)

Task 4.5 Finalize Design Vector

Inputs:

The inputs to Task 4.5 are the baseline design vector and the filtered set of survivability design variables. Feedback from the model development may inform changes to the design vector. Iterative changes to the design vector may also be required following completion of the tradespace analysis.

Outputs:

The output of Task 2.4 is the finalized design vector, including enumeration and sampling strategies.

Description:

Finalizing the design variables is required before modeling and simulating the design alternatives. 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 associated with 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).

Dependencies:

Inputs: 2.4, 4.4, 5.1, 5.2, 5.4, 8.1
Outputs: 5.1, 5.2, 5.3, 6.1, 6.2, 6.3

Space Tug Example:

See Table 5-5. Space Tug Design Options (n=2560)

Phase 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 vectors 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

Inputs:

Decomposing the model code requires a finalized set of attributes, the finalized design vectors, and physical knowledge of the relationship between the design variables and attributes. Although the disturbance models are not integrated into the model until Phase 6, the system-independent models of disturbance occurrence developed in Task 3.3 are also consulted to inform the software architecture.

Outputs:
The output of Task 5.1 is a list of software modules and an N-squared matrix describing the inputs and outputs of each module.

Description:
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. Modules within the matrix enable the model to be decomposed to enable parallel development.

Dependencies:
Inputs: 1.3, 2.2, 2.3, 2.4, 3.3, 4.3, 4.5, 5.2, 6.1, 6.2, 6.3
Outputs: 2.4, 5.2, 5.3, 6.1, 6.2, 6.3

Space Tug Example:
See Table 6-3 for an n-squared matrix representation of the space tug software architecture.

Task 5.2 Translate Design Vectors to Attributes

Inputs:
The sampled design variables are input to the performance model to calculate the attributes of the multi-attribute utility function.

Outputs:
The output of Task 5.2 is the calculated performance of each design vector in each attribute.

Description:
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.

Dependencies:
Inputs: 1.3, 2.1, 2.3, 4.5, 5.1
Outputs: 2.3, 2.4, 4.5, 5.1, 5.4, 6.1, 6.2, 6.3

Space Tug Example:
As documented in McManus and Schuman (2003), a simple performance model translates the space tug design vectors to attributes. For example, the ΔV attribute is computed from the rocket equation.

Task 5.3 Translate Design Vectors to Lifecycle Cost

Inputs:

The sampled design variables are input to the cost model to calculate the attributes of the tradespace. Task 5.3 may also require input from Task 6.3 if the system incurs costs associated with recovery operations.

Outputs:

The output of Task 5.3 is an estimate of the lifecycle cost of the design vectors.

Description:

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 (Wertz and Larson 1999).

Dependencies:

Inputs: 2.1, 4.5, 5.1, 6.3
Outputs: 5.1, 8.1

Space Tug Example:

The launch and first-unit hardware procurement costs for space tug are estimated using the vehicle wet and dry masses (calculated in the model as intermediate variables) and assuming $20,000/kg in cost for wet mass and $150,000/kg in cost for dry mass.

Task 5.4 Apply Multi-Attribute Utility Function

Inputs:

The inputs to Task 5.4 are the multi-attribute utility function elicited from the decision-maker and the attribute values calculated for each design vector.

Outputs:

The output of Task 5.4 is a utility value for each design vector representing the benefit delivered to the decision-maker in a nominal environment.

Description:

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.

Dependencies:

Inputs: 1.3, 5.2
Outputs: 4.5, 6.4, 8.1

Space Tug Example:

Figure 5-6. Baseline MATE Tradespace shows the calculated utility values for each space tug alternative and plots them against cost.

Phase 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 dynamically characterizing system performance from a path-dependent, 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

Inputs:

The inputs to Task 6.1 include the system-independent models of the disturbance environment and the finalized design vector.

Outputs:

The output of Task 6.1 is a set of disturbances and associated times of impact events for each run of the susceptibility model across the tradespace.

Description:

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), 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.

Dependencies:

Inputs: 3.3, 4.3, 4.5, 5.1
Outputs: 5.1, 6.2

Space Tug Example:

See Figure 5-9. Conjunction Outcomes.

Task 6.2 Model Probabilistic Vulnerability

Inputs:

The inputs to Task 6.2 are the system-dependent disturbances in a given run of the simulation, their associated time-stamps, and the survivability design variables in the finalized design vector.

Outputs:

The output of Task 6.2 is a series of time-stamped utility losses for each run of the simulation which characterize degradation of system attributes in the disturbance environment.

Description:

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. The vulnerability model takes the form of a probabilistic lottery in which multiple runs are required to extract the distribution of potential outcomes. Although static, the vulnerability model is only activated 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.

Dependencies:

Inputs: 3.3, 4.3, 4.5, 5.1, 6.1
Outputs: 5.1, 6.3, 6.4

Space Tug Example:

See Table 5-6. Debris Impact Outcomes.

Task 6.3 Model Probabilistic Recovery

Inputs:

The key input to Task 6.3 are the survivability design variables in the finalized design vector and the outcomes of disturbance impacts from the vulnerability model.

Outputs:

The output of Task 6.3 is a series of time-stamped utility gains (and any associated costs) for each run of the simulation with recovery operations.

Description:

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 takes the form of 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.

Dependencies:

Inputs: 4.3, 4.5, 5.1, 6.2
Outputs: 5.1, 5.3, 6.4

Space Tug Example:

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. A given servicing mission is assumed to have a 70% success rate with response times lognormally distributed (with a mean of six months and a standard deviation of a year).

Task 6.4 Generate Distributions of Utility Trajectories

Inputs:

The inputs to Task 6.4 are the critical value thresholds and permitted recovery times elicited from the decision-maker, the beginning-of-life utility for design alternative, and the perturbations of utility over the lifecycle as provided by the survivability models.

Outputs:

The outputs of Task 6.4 are utility trajectories of each design alternative in each run of the Monte Carlo simulation.

Description:

As defined in Chapter 3, 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 incorporates 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.

Determining the appropriate number of Monte Carlo trials requires a trade-off between the accuracy of the reported survivability metrics and computing time (Hazelrigg 1996). To determine the number of runs, it is advisable to conduct a convergence study on a small number of design vectors to examine the sensitivity of the reported survivability metrics to the number of Monte Carlo trials. Precisely understanding the variance of the reported survivability metrics is particularly critical if the tear tradespace is subsequently filtered for Pareto efficiency.

Dependencies:

Inputs: 1.4, 1.5, 5.4, 6.2, 6.3
Outputs: 7.1, 7.2, 7.3

Space Tug Examples:

See Figure 5-13. Sample Utility Trajectory Outputs from Design Vectors 19 and 1137 and Figure 6-5. Monte Carlo Convergence for One Design Vector.

Phase 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.

Task 7.1 Establish Percentile Reporting Levels

Inputs:

The inputs to Task 7.1 are the utility trajectory distributions. Establishing percentile reporting levels may also incorporate feedback from subsequent tradespace analysis.

Outputs:

The outputs of Task 7.1 are the percentile reporting levels for the distributions of time-weighted average utility and of threshold availability.

Description:

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 and threshold availability, introduced in Chapter 3, 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 an 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 itself through the selection of lower percentiles). Selection of the percentile reporting levels is an iterative process with Task 8.1, Conduct Integrated Tradespace Exploration.

Dependencies:

Inputs: 6.4, 8.1
Outputs: 7.2, 7.3

Space Tug Example:

In the space tug example, the median (50th percentile) is selected for time-weighted average utility and the 5th percentile is selected for threshold availability. These selections improve data visualization since the survivability metrics varied over the tradespace at these reporting levels. Additionally, decision-makers are likely to be more risk-averse regarding threshold availability (a construct for measuring assured access to some level of minimum capability) than time-weighted average utility (a construct for assessing degree of degradation).

Task 7.2 Calculate Time-Weighted Utility and Threshold Availability

Inputs:

The inputs to Task 7.2 are the utility trajectories and the percentile reporting levels.

Outputs:

The outputs of Task 7.2 are the probabilistic survivability metrics of time-weighted average utility and of threshold availability.

Description:

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.

Dependencies:
Inputs: 6.4, 7.1
Outputs: 8.1

Space Tug Example:
See Figure 5-14. Distributions of Time-Weighted Average Utility and Figure 5-15. Sample Distribution of Threshold Availability.

Phase 8: Explore Tradespace

Having applied the survivability metrics, 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 Cost, Utility, and Survivability Trades

Inputs:
The inputs to Task 8.1 are the calculated values for lifecycle cost, design utility, time-weighted average utility/utility loss, and threshold availability.

Outputs:
The direct output of Task 8.1 is a broad understanding of the tradespace to inform selection of a subset of designs for more detailed analysis. However, insights gathered from tradespace exploration may also cause the decision-maker to relax constraints on the design space (Task 2.1) and modify the percentile reporting levels of the survivability metric (Task 7.1). In addition, if the design alternatives fail to meet stakeholder needs and expectations (*e.g.*, sparse tradespace), the analyst may be inspired to consider new design concepts (Task 2.2) and survivability strategies (Tasks 4.1 and 4.5).

Description:
The purpose of tradespace exploration is to map the decision-maker preferences in the value domain onto the space of possible designs in the technical 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 identified for more detailed analysis.

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 tradespace representation. Decision-makers may navigate the tradespace by examining designs near the top-left (high utility, low cost) with high availability (darker) and minimal utility loss (shorter tail).

Dependencies:
Inputs: 5.3, 5.4, 7.2
Outputs: 2.1, 2.2, 4.1, 4.5, 7.1, 8.2

Space Tug Example:

Figure 6-6 presents a survivability tear tradespace from space tug in which designs at the Pareto-surface of cost, utility, and utility loss are displayed.

Task 8.2 Select Designs for Further Analysis

Inputs:
The inputs to Task 8.2 are decision-maker insights from the tradespace.

Description:
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 small number of design vectors for higher-fidelity modeling. To assess how the various survivable concepts perform, response surfaces may also be drawn to show how the survivability design variables affect performance across the survivability metrics. This analysis may be conducted on specific designs for prescriptive insights as well as to the entire tradespace to show larger trends.

Dependencies:
Inputs: 8.1

Space Tug Example:

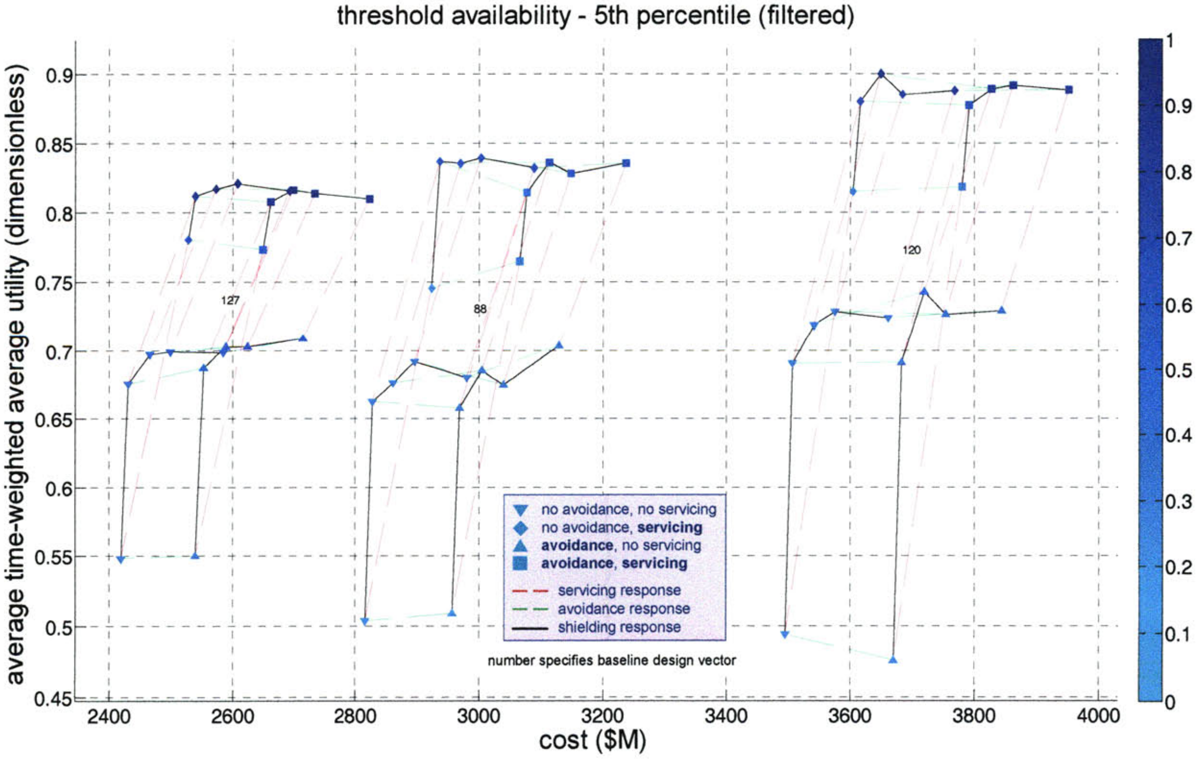


Figure 9-9. Survivability Response Surfaces for Large Space Tugs

Appendix F. Tradespace Plots of Satellite Radar

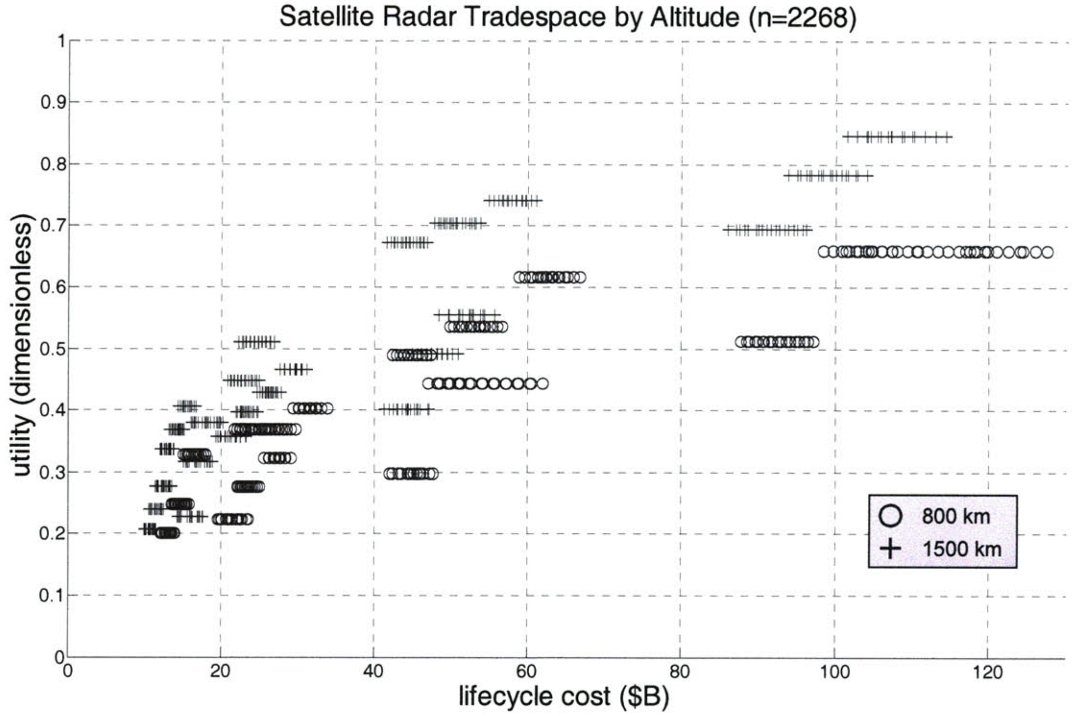


Figure 9-10. Effect of Orbit Altitude on Baseline SR Tradespace

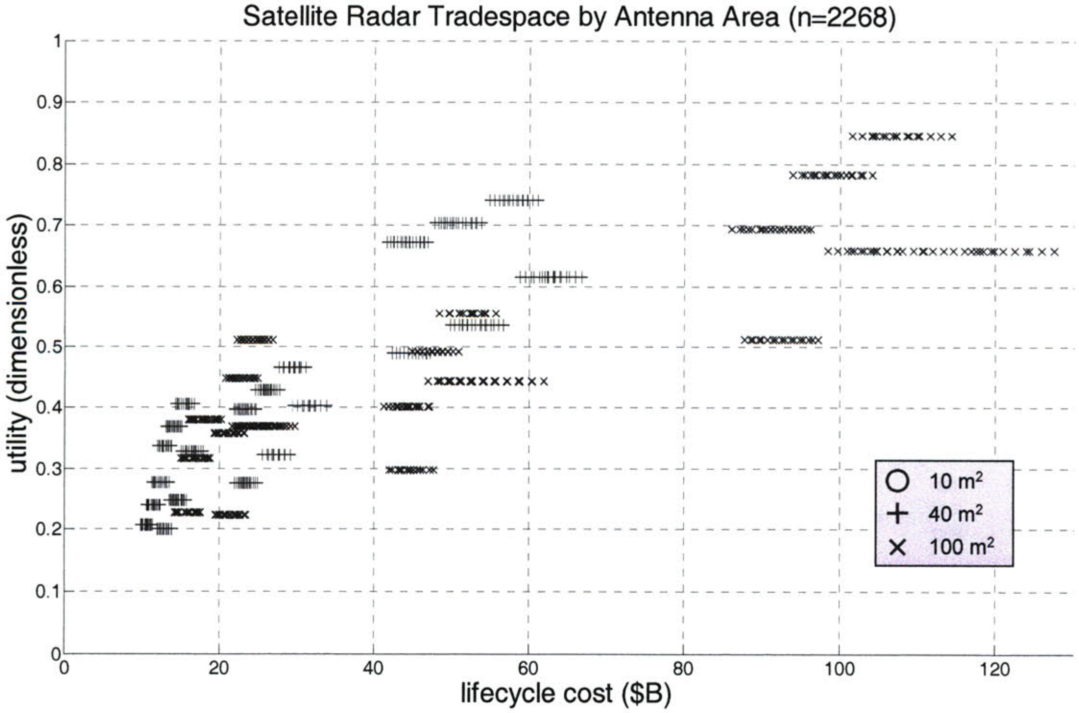


Figure 9-11. Effect of Antenna Area on Baseline SR Tradespace

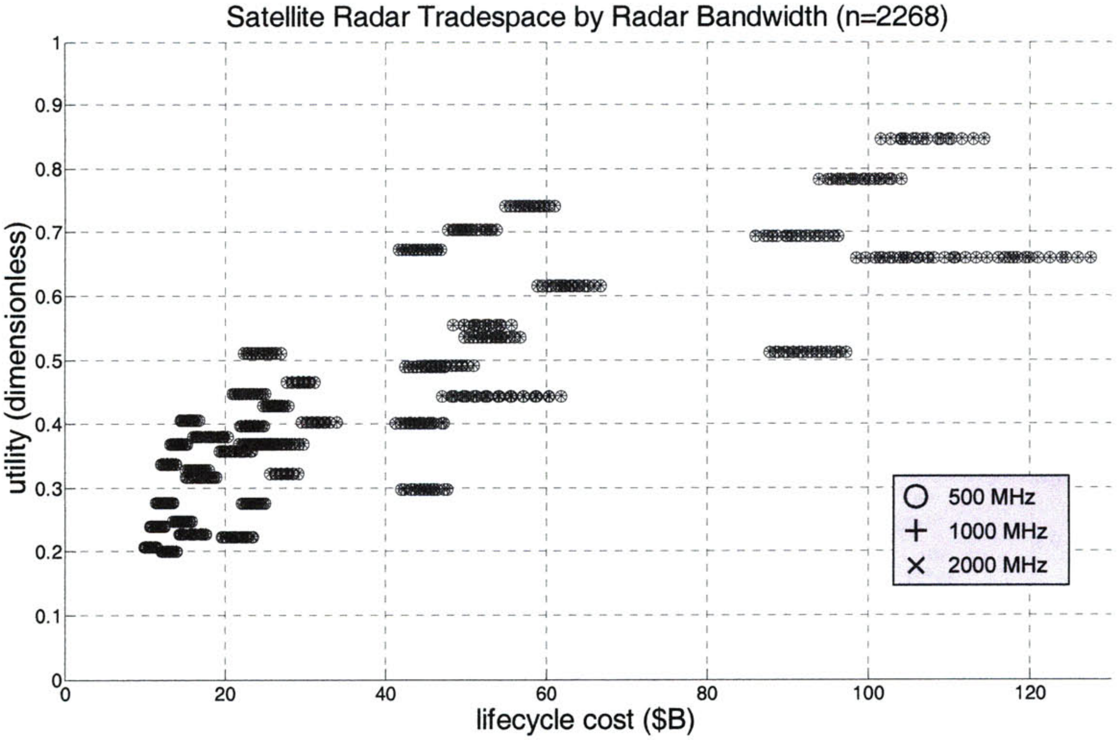


Figure 9-12. Effect of Radar Bandwidth on Baseline SR Tradespace

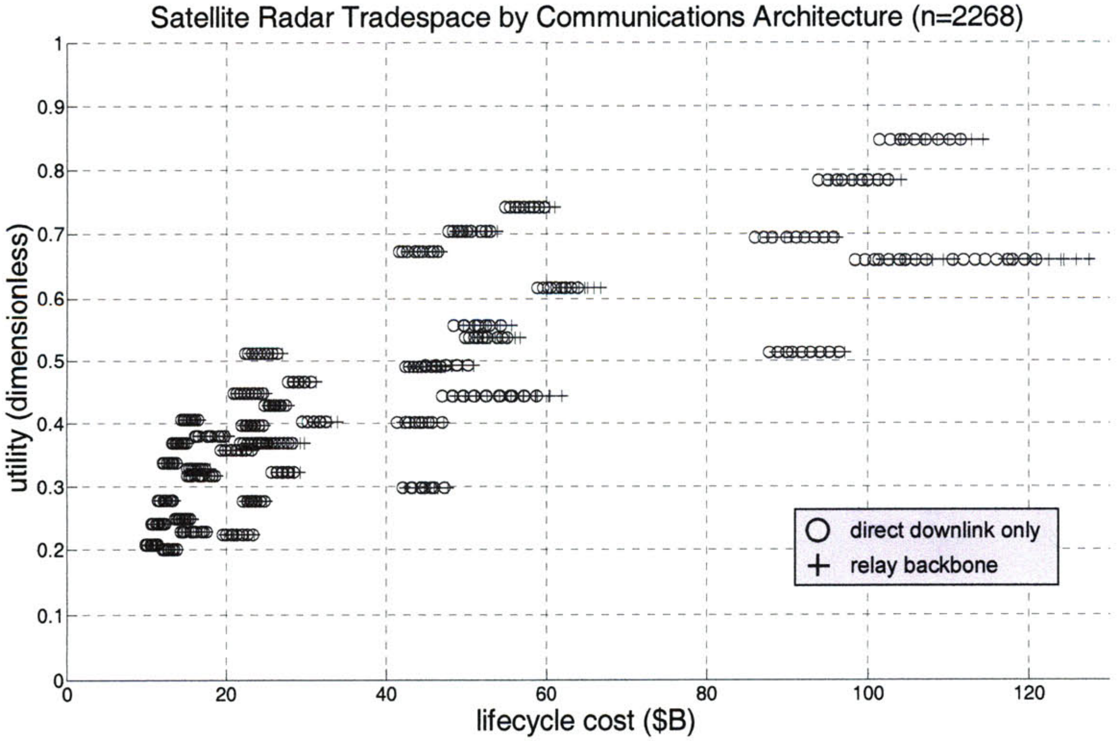


Figure 9-13. Effect of Communications Architecture on Baseline SR Tradespace

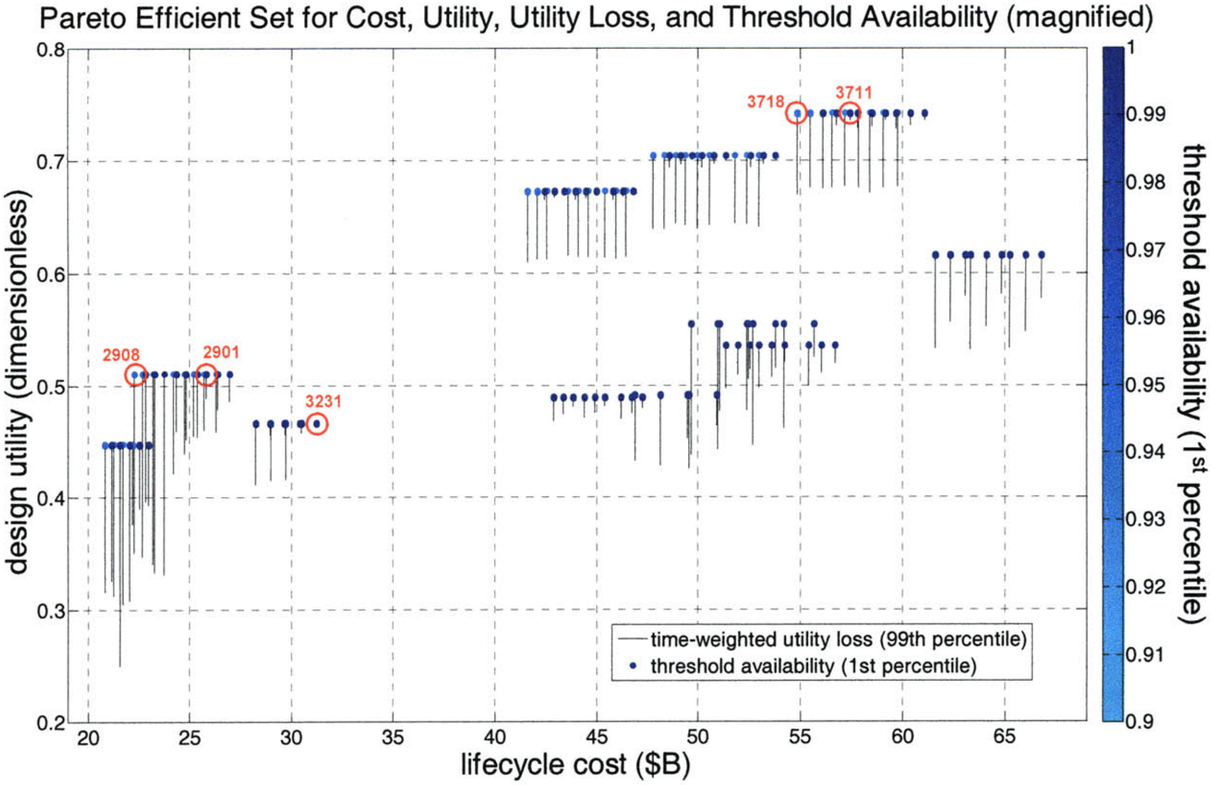


Figure 9-14. Magnified and Filtered Survivability Tear Tradespace - Risk Averse Decision-maker