Two Empirical Tests of Design Principles for Survivable System Architecture

Matthew G. Richards
Massachusetts Institute of Technology
77 Massachusetts Ave., Bld. NE20-343
Cambridge, MA 02139
mgr@mit.edu

Adam M. Ross
Massachusetts Institute of Technology
77 Massachusetts Ave., Bld. NE20-388
Cambridge, MA 02139
adamross@mit.edu

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

Donna H. Rhodes
Massachusetts Institute of Technology
77 Massachusetts Ave., Bld. NE20-388
Cambridge, MA 02139
rhodes@mit.edu

Abstract. Survivability, the ability of a system to minimize the impact of a finite-duration disturbance on value delivery, is increasingly recognized beyond military contexts as an enabler for maintaining system performance in the presence of dynamic disturbance environments. This paper attempts to validate a preliminary set of twelve general design principles for survivability through two empirical tests. Survivability features of the A-10A "Warthog" combat aircraft and UH-60A Blackhawk helicopter, two systems designed for reduced vulnerability, are inductively traced to an existing set of principles. Seven unique insights are derived from the analysis, and the design principles are revised to reflect the lessons learned. A new set of seventeen design principles are formalized: six aimed at reducing susceptibility and eleven aimed at reducing vulnerability. The paper concludes with propositions for future work for developing a theory of survivable system architecture and a discussion of the importance of empiricism in systems engineering.

Introduction

In addition to meeting requirements in a static context, the performance of system architectures is increasingly defined by an ability to deliver value to stakeholders in the presence of changing operational environments, economic markets, and technological developments. Research on system changeability and uncertainty management has been conducted as a first step towards the achievement of such value robustness (de Weck, de Neufville et al. 2004; Fricke and Schulz 2005; McManus and Hastings 2006; Ross 2006; Ross and Hastings 2006; Nilchiani and Hastings 2007). For example, Ross (2006) develops a descriptive theory of the temporal systems property changeability, a subset of the "ilities" (*i.e.*, flexibility, adaptability, rigidity, robustness, scalability, and modifiability) as well as prescriptive tradespace metrics to operationalize the theory for conceptual design. In an attempt to improve and build upon the existing theory of *changeability*, ongoing research on system survivability is focused on particular challenges posed by dynamic disturbance environments and on how survivability might be better articulated, evaluated, and implemented during the conceptual design of engineering systems.

The operational environment of engineering systems is increasingly characterized by disturbances that may asymmetrically degrade performance, particularly for systems with networked structures. Examples of impulse events triggering catastrophic losses include the tragic events of September 11th, 2001 (Kean, Hamilton et al. 2004), the Northeast Blackout of 2003 (Abraham and Efford 2004), and Hurricane Katrina (Knabb, Rhome et al. 2005). More recently, 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).

Despite growth in the scope, frequency, and magnitude of disturbances, a 2000 report for the U.S. Army Research Laboratory on systems and networks with critical survivability requirements draws several troubling conclusions (Neumann 2000). In particular, inadequacies are identified in the ability of systems engineers and architects to manage such risks. Existing criteria and systems architecting methodologies for evaluating highly survivable systems and networks are found to be "incomplete and inadequate." Furthermore, it is noted that there is "almost no experience in evaluating systems having a collection of independent criteria that might contribute to survivability" nor in examining the interactions among different criteria. These shortcomings make it difficult to specify, develop, procure, operate, and maintain systems with critical survivability requirements.

In addition to being a poorly understood system property, survivability at the architecture level is further complicated when issues extending beyond design of the technical system are internalized, such as operational behavior, human factors, and supporting infrastructures (Hollnagel, Woods et al. 2006). Although survivability is an emergent system property that arises from interactions among components and between systems and their environments, 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 domain-specific operating scenarios and presupposed disturbances rather than a general theory with indeterminate threats. As a result, current models provide limited insights for senior decision makers, who trade system survivability with cost and utility during conceptual design. Development of a generic survivability framework and associated design methodologies represent both a need and an opportunity for growth within systems engineering.

Three sections compose the body of the paper. First, preliminary results of a theory of survivable systems architecting are presented. These preliminary results include a value-centric definition and conceptualization of survivability, a generic framework for analyzing system interactions with natural and synthetic hostile environments, and a set of twelve design principles for the achievement of survivable system architecture (Richards, Hastings et al. 2007; Richards, Ross et al. 2007). Second, the validity of the twelve design principles—deduced from the generic survivability framework—is explored through a series of empirical tests. In particular, survivability features in two existing aerospace systems—the A-10A Thunderbolt II combat aircraft and UH-60A Blackhawk helicopter—are traced to the set of twelve general design principles. Third, the results of this inductive mapping are integrated into the existing theory. A need to expand the survivability framework is discussed, and new design principles are identified. The paper concludes with a discussion of the value of empirical research in systems engineering and of the implications of the updated theory for architecting survivable systems.

Survivability Theory Development

Survivability Definition

Success of a system is dependent on how much value it is perceived to deliver to its stakeholders. Value, in this sense, is considered to be synonymous with net benefit (*i.e.*, received benefits less costs for receiving those benefits). 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. Taking the value-centric perspective, system designers are freed to consider multiple paths to achieve the same value delivery (Ross 2006). The multi-path view is useful for considering survivability issues when original value delivery mechanisms may be blocked by a disturbance.

Given that all systems exist to deliver value, a value-centric definition of survivability has the additional advantage of achieving domain neutrality. Another desirable attribute of a survivability definition is an internalization of temporal properties because survivability is an aggregate system property that reveals itself over time. 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.

As discussed in Ball's (2003) formulation for aircraft combat survivability, design for survivability may be approached in terms of reducing susceptibility, and in terms of reducing vulnerability. Survivability may be achieved through either (1) the reduction of the likelihood or magnitude of a disturbance, Type I survivability, or (2) the satisfaction of a minimally acceptable level of value delivery during and after a finite disturbance, Type II survivability.

Figure 1 illustrates Type I and Type II survivability across two *epochs*, time periods of a fixed context (Ross 2006). Type I survivability, appearing as a dashed horizontal line, is achieved if the disturbance never reduces the delivered value [V(t)] below the required value threshold [V_x]. Type II survivability is more involved: Following successful value delivery during Epoch 1a, the system experiences a finite-duration disturbance during Epoch 2 that degrades performance. Once the disturbance ceases, the environment reverts back to the original context, Epoch 1b. In order to determine whether the system is survivable, several factors must be defined: the minimum acceptable value to be delivered during the disturbance [V_e], the permitted recovery time elapsed past the onset of the disturbance [T_r], the minimum acceptable recovered value after the recovery period is complete [V_x]. In Figure 1, the system achieves Type II survivability by maintaining value delivery [V(t)] at a level above the emergency value threshold [V_e] and then recovering to deliver value above the required value threshold [V_x] within the permitted recovery time [T_r].

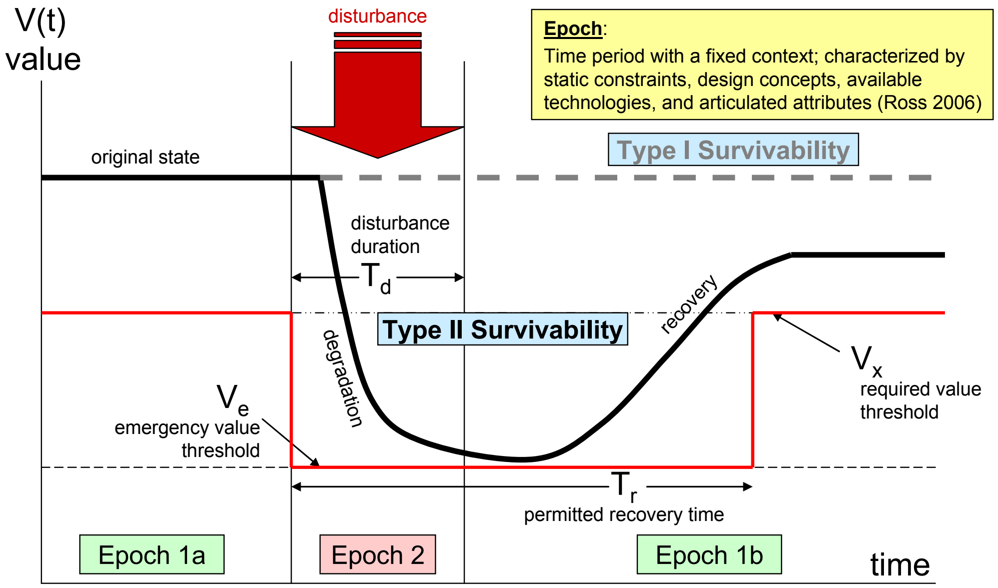

Figure 1. Definition of Survivability

Survivability Framework

Having established a definition of survivability, a preliminary framework was developed for visualizing and deriving design principles of survivability (Figure 2). Consisting of the minimum set of elements needed to describe the interaction between a system and a given hostile environment, the framework includes 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 survivability.

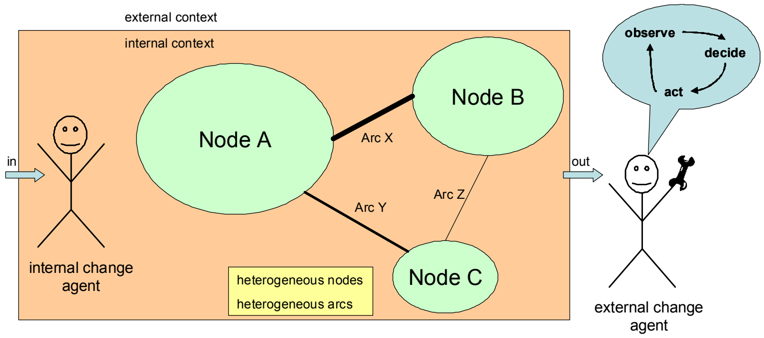

Figure 2. Generic System-Disturbance Representation

The external change agent in Figure 2 is an abstraction of a source of disturbances, whether 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 utility-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.) 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.

Preliminary Design Principles

Utilizing the framework discussed above, twelve design principles for enhancing survivability were enumerated (Richards, Ross et al. 2007). For example, 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. In total, six design principles for enhancing Type I survivability were initially identified: (1.1) prevention, (1.2) mobility, (1.3) concealment, (1.4) deterrence, (1.5) preemption and (1.6) avoidance. Six design principles for enhancing Type II survivability were also enumerated: (2.1) hardness, (2.2) evolution, (2.3) redundancy, (2.4) diversity, (2.5) replacement, and (2.6) repair. Table 1defines each of these principles and Figure 3 illustrates how each of these twelve design principles may positively affect value during a disturbance lifecycle.

Table 1. Preliminary 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
2.5	**replacement**	substitution of system elements to improve value delivery
2.6	**repair**	restoration of system to improve value delivery

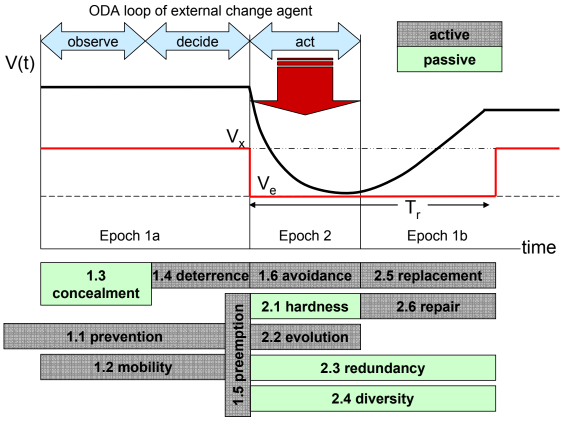

Figure 3. Mapping of Design Principles to Disturbance Lifecycle

Survivability Design Principles: Two Empirical Tests

The previous section described how design principles of survivability were deductively enumerated from an abstract theoretical framework consisting of the minimum set of elements needed to characterize the interaction between a system and a given hostile environment. In this section, the validity of these results is empirically tested through an inductive mapping of survivability features on existing systems to the set of design principles. Following an overview of the methodology used to trace domain-specific instantiations of survivability features to the general principles, results from two systems are presented: (1) the A-10A Thunderbolt II combat aircraft and (2) the UH-60A Blackhawk helicopter.

Methodology

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 this work, the purpose of empirical testing is to check for completeness, logical consistency, and taxonomic precision of the survivability framework. 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).[1]

The process of empirically testing the survivability design principles begins by attempting to establish traceability from survivability features in operational systems to the twelve general 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 the following sections, matrices are used to qualitatively illustrate traceability 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 twelve preliminary 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 were shaded in grey. These grey regions will be subjected to more rigorous analysis and will potentially inform improvements to the existing design principle set.

In selecting systems for the inductive mapping, three factors were considered: (1) the disturbance environments associated with a system's operational context, (2) access to data regarding system survivability features, and (3) striking an appropriate balance between depth and breadth for a conference paper. Given these factors, two aerospace systems—a combat aircraft and a military helicopter—were selected for the empirical tests.[2]

Test #1 – A-10A Thunderbolt II Aircraft

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,

[1] 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, W. (2006). Social Research Methods. Boston, Pearson.

[2] In testing the design principles against the A-10A and UH-60A, the unit of analysis is a piloted 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).

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.

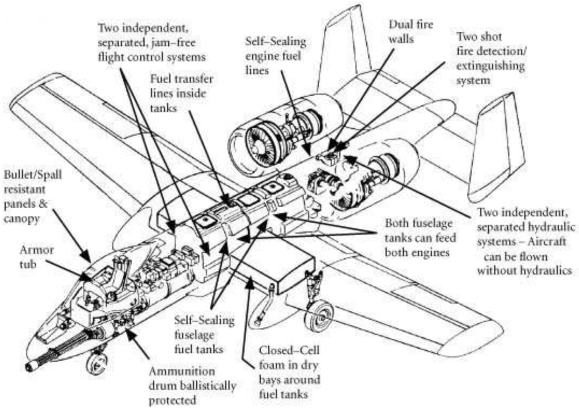
Two independent, separated, jam–free flight control systems
Self–Sealing engine fuel lines
Dual fire walls
Two shot fire detection/ extinguishing system
Fuel transfer lines inside tanks
Bullet/Spall resistant panels & canopy
Armor tub
Both fuselage tanks can feed both engines
Two independent, separated 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 4. 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 4 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.

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 general design principles. Table 2 below 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 unique insights emerged. The first relates to the definition of *redundancy*. Moving down Table 2 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 2 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).

Table 2. Tracing of A-10A "Warthog" Survivability Features to Design Principles

		Type I (Reduce Susceptibility)						Type II (Reduce Vulnerability)					
	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							

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 inability to trace the A-10's situational awareness features to either the design principle set or survivability framework suggests an incompleteness in the generic system-disturbance representation in Figure 2, which includes an ODA loop for the external change agent but not for the internal change agent.

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, 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.

Test #2 – UH-60A Blackhawk Helicopter

The UH-60A Blackhawk is a medium-lift utility or assault helicopter used by the U.S. Army and over 20 military services around the globe. As a tactical transport, the UH-60A lift capability can accommodate a fully-equipped 11-person infantry squad or a 105 mm Howitzer, its crew of six, and 30 rounds of ammunition (USA 2006). Just as the A-10 was developed to address the vulnerabilities of the Air Force's fixed-wing aircraft in Vietnam, 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 5 illustrates some of its vulnerability reduction features,

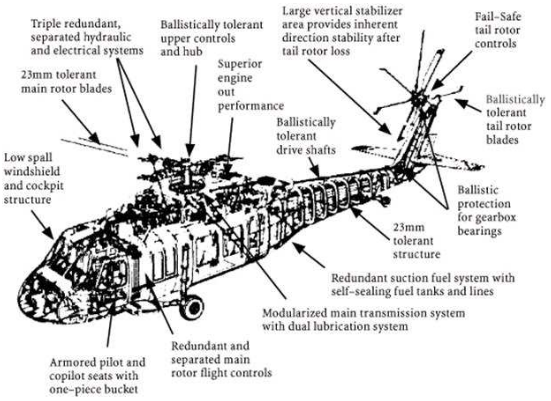
Triple redundant, separated hydraulic and electrical systems
Ballistically tolerant upper controls and hub
Large vertical stabilizer area provides inherent direction stability after tail rotor loss
Fail-Safe tail rotor controls
23mm tolerant main rotor blades
Superior engine out performance
Ballistically 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 5. Some Vulnerability Reduction Features on the UH-60 Blackhawk (Ball 2003)

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).

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 3 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 framework. Three potentially new design principles are discussed to account for these discrepancies. Also, problems with mapping five other survivability features were repeats of problems uncovered during the A-10 mapping.

The first row of Table 3, "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 twelve 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 unique insight 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 unique insight: the need for *containment* as a new Type II design principle. By incorporating the survivability 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.

Table 3. Tracing of UH-60A Blackhawk Survivability Features to Design Principles

		Type I (Reduce Susceptibility)						Type II (Reduce Vulnerability)					
	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							

In addition to the three unique insights uncovered above, the Blackhawk test case also exposed two problematic aspects of the preliminary survivability framework that were previously discussed in the A-10 test case: (1) the need to decompose the design principle of diversity into *heterogeneity* and *distribution* and (2) the need to distinguish between *redundancy* and *margin*. Five UH-60A examples of the diversity distinction 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. Two examples of the redundancy/margin distinction include [rotor blade and drive train] operates 1+ hours after loss of all oil and [propulsion] good one engine out capability.

Results

In developing a set of general survivability design principles, there is an inherent tension among competing desires for clarity, mutual independence, collective exhaustiveness, and maintaining a tractable number of principles. The process of attempting to trace the survivability features of the A-10A combat aircraft and 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 A-10A and UH-60A were successfully mapped to the existing survivability framework and design principles. The size of the set of Type II design principles was expanded by five and limitations with the survivability framework and definitions of some design principles were discovered (Table 4). The implications of each of the problems enumerated in Table 4 need to be considered for validating and improving the proposed set of design principles and survivability framework.

Table 4. Seven Insights form A-10 and UH-60 Test Cases

Problem		Implication
1	Survivability features that employ design margin are untraced (A-10, UH-60)	Add new Type II design principle of margin
2	Situational awareness features do not employ any existing design principles (A-10)	Add ODA loop to internal change agent in survivability framework
3	Imprecise definition of diversity – includes both characteristic and spatial (A-10, UH-60)	Decompose diversity into heterogeneity and distribution
4	Redundancy definition is physically constructed (A-10)	Define redundancy functionally
5	Survivability features that reduce the number of system failure modes are untraced (UH-60)	Add new Type II design principle of failure mode reduction
6	Survivability features employing "physics-of-failure" are untraced (UH-60)	Add new Type II design principle of fail-safe
7	Survivability features that limit or slow the propagation of failures are untraced (UH-60)	Add new Type II design principle of containment

Synthesis

Integrating the results of the inductive mappings of the A-10 and UH-60 into the existing theory requires an expansion of the survivability framework (Figure 2) and design principle set (Table 1). While changes to the design principles were an expected outcome of the empirical tests, changes to the generic representation of system-disturbance interactions were not anticipated.

For the survivability framework, the inability to trace the A-10 survivability features relating to situational awareness exposed a missing element: an observe, decide, act loop for the internal change agent. An ODA loop is essential for modeling the process of a system operator utilizing active survivability principles. Whether employing human-in-the-loop or artificial control, the abilities to receive information regarding system and environmental conditions and to make decisions with such information are prerequisites for taking action. Although the presence of an ODA loop for the internal change agent was recognized in the initial construction of the survivability framework, it was (mistakenly) excluded from the generic system-disturbance representation (based on an assumption that it would not be useful in the enumeration of design principles).

Table 5. Revised 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 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
2.10	replacement	substitution of system elements to improve value delivery
2.11	repair	restoration of system to improve value delivery

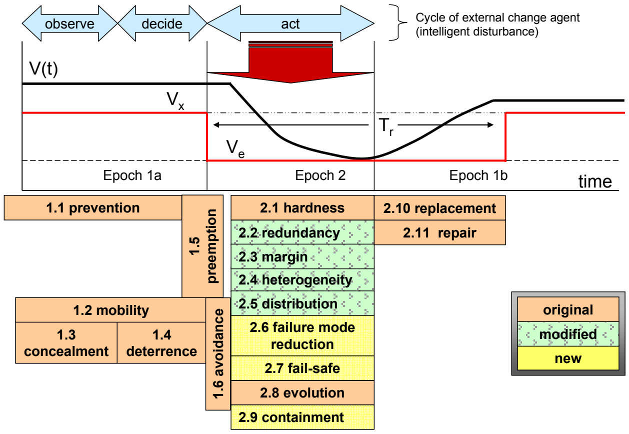

Figure 6. Mapping of Design Principles to Disturbance Lifecycle (revised)

Comparing Table 1 to Table 5 shows the extensive modifications required of the Type II survivability set to accommodate the results of the empirical tests: the revision of the definition of redundancy (2.2); the decomposition of diversity into the design principles heterogeneity (2.4) and distribution (2.5); the distinction drawn between redundancy and margin (2.3); 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. Figure 6 depicts the time intervals during which each of the seventeen design principles may positively affect value delivery during a disturbance lifecycle. Principles enhancing Type I survivability add value before a disturbance impacts a system while Type II principles add value following a disturbance impact.

Given the extensive modifications required of the preliminary survivability framework and design principles following two empirical tests, an obvious next step is to conduct more empirical tests of existing systems. Recognizing that both the A-10A and UH-60A were designed for low vulnerability—and that every design principle modification involved Type II survivability—it is especially important to explore systems designed for low susceptibility to target validation in the Type I design principles. Furthermore, future empirical tests might extend beyond the discipline of survivability engineering and the aerospace domain. Interdisciplinary research, incorporating safety and security engineering, might enable the application of existing architectural approaches to new areas. For example, the design principle of failure mode reduction—the elimination of system failure modes through substitution, simplification, decoupling, and reduction of hazardous materials or conditions—employs the same techniques as hazard reduction in system safety engineering (Leveson 1995). Exploring highly survivable systems outside of the aerospace domain, such as biological systems or resilient computer networks, might reveal similar insights (*e.g.*, design principle of containment analogous to employment of tourniquets in emergency bleeding control).

As more systems are inductively mapped to the design principles, an opportunity to construct a morphological matrix of potential survivability features for each design principle presents itself. Inverting the bottom-up mapping of features to principles, such a top-down analysis integrated across multiple systems might be a powerful tool for system architects to consider a large set of survivability features for each phase in the lifecycle of a disturbance.

Conclusion

The process of tracing survivability features of real systems to the design principles and the subsequent improvements made to the theory illustrate 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 abstract concepts and theoretical relationships. Following generation of a set of hypotheses (*i.e.*, the original twelve design principles), an experiment was conducted (*i.e.*, tracing of survivability features of existing systems to design principles). Based on the results of the experiment, a new set of hypotheses were proposed (*i.e.*, new set of seventeen design principles) for subsequent testing. By attempting to validate the preliminary survivability framework using inductive methods, this paper successfully applied concrete empirical evidence from the A-10A and UH-60A, revealing insights for a more general theory of survivable system architecture.

The scope of this paper—the refinement of a set of design principles for survivable system architectures—addresses one aspect of an integrated effort to improve the articulation, evaluation, and implementation of survivability during the conceptual design of engineering systems. A next step of the research will involve the construction of a quantitative implementation of the design principles into a simulation-based dynamic tradespace exploration approach for comparing designs on the basis of their survivability. The design principles will be used to expand the set of system design trade-offs under consideration. Future work will address the need for improvements in evaluating survivability as a stochastic dependent variable and developing metrics for survivability in dynamic tradespaces.

Acknowledgements

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

References

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

Ball, R. (2003). The Fundamentals of Aircraft Combat Survivability Analysis and Design. 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.

Clausing, D. and D. Frey (2005). "Improving System Reliability by Failure-Mode Avoidance Including Four Concept Design Strategies." *Systems Engineering,* 8(3): 245-261.

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.

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.

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.

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

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.

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

Leveson, N. (1995). Safeware: System Safety and Computers. Boston, Addison-Wesley.

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.

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.

Osinga, F. (2006). Science, Strategy and War: The Strategic Theory of John Boyd. London, UK, Routledge.

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

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

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 (2006). "Assessing Changeability in Aerospace Systems Architecting and Design Using Dynamic Multi-Attribute Tradespace Exploration." *AIAA Space 2006*, San Jose, CA.

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."

Smallwood, W. (1993). Warthog: Flying the A-10 in the Gulf War. Dulles, Potomac Books.

USA (2006). "The UH-60A Black Hawk." *U.S. Army Aviation Warfighting Center*.

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.

Biographies

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

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

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

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