Empirical Validation of Design Principles for Survivable System Architecture

Matthew G. Richards, Adam M. Ross, Daniel E. Hastings, and Donna H. Rhodes
Massachusetts Institute of Technology
77 Massachusetts Ave., Building NE20-388
Cambridge, MA 02139
http://seari.mit.edu

Abstract *– Survivability, the ability of a system to minimize the impact of a finite-duration disturbance on end-user value delivery, is increasingly recognized beyond military contexts as an enabler of maintaining system performance in operational environments characterized by dynamic disturbances. Seventeen general design principles are proposed to inform concept generation of survivable system architectures. Six of these design principles focus on a survivability strategy of susceptibility reduction: (1.1) prevention, (1.2) mobility, (1.3) concealment, (1.4) deterrence, (1.5) preemption, and (1.6) avoidance. Eleven of the principles focus on vulnerability reduction: (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, (2.9) containment, (2.10) replacement, and (2.11) repair. In this paper, the completeness, taxonomic precision, and domain-specific applicability of the design principle framework is empirically tested through case applications to survivability features of the F-16C combat aircraft and Iridium satellite system. Integrating results of these two tests with previous tests (e.g., UH-60A Blackhawk helicopter, A-10A aircraft), the validity of the design principle framework for aerospace systems is demonstrated.*

Keywords *– survivability engineering, concept generation, value-based design, robust design, risk management*

I. INTRODUCTION

Survivability is the ability of a system to minimize the impact of a finite-duration disturbance on value delivery [1]. Design for survivability may be approached in terms of reducing susceptibility (Type I survivability) and in terms of reducing vulnerability (Type II survivability). Traditionally specified as a requirement in military systems [2], survivability is an increasingly important attribute of all systems which must be robust to environments characterized by system-threatening hazards [3]. While disturbances may originate from a wide range of man-made and natural environments, a universal challenge confronting system architects is the specification, development, procurement, operation, and maintenance of systems with critical survivability requirements [4].

The design principles analyzed in this research are intended to improve the conceptual design of survivable systems by enhancing concept generation activities—expanding the set of system design trade-offs under consideration. While selected domains such as combat aircraft engineering have developed a variety of methods and tools to evaluate the survivability of alternative concepts [5], the literature offers far less insights regarding the generation of alternatives. This is a significant gap given the criticality of front-end systems engineering activities (during which management leverage is highest and the majority of development resources tend to be committed) [6].

Work related to this research includes the development of survivability enhancement concepts for combat aircraft [7], the application of survivability principles from biological systems to the design of networked services [8], and the extraction of robust design strategies from the U.S. patent database [9]. However, the survivability design principles proposed in this research address different questions. In contrast to the two former research areas on combat aircraft and network design, the design principles in this paper are constructed for general applicability rather than for systems within a particular domain. The design principles in this paper are distinguished from the latter research on 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.

Five sections compose the paper. Following this introduction, the second section presents preliminary results of a theory of survivable systems architecting. 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 seventeen design principles for the achievement of survivable system architecture [10]. In the third section, the validity of the seventeen design principles—derived from the generic survivability framework and empirical tests involving the A-10 Thunderbolt II combat aircraft and UH-60A Blackhawk helicopter—is explored through inductive methods. In particular, survivability features in two additional systems that have operated in harsh environments—the F-16 combat aircraft and Iridium satellite system—are traced to the set of seventeen general design principles. In the fourth section, the four empirical tests as a whole are discussed—including implications for both aerospace and non-aerospace systems. After summarizing the analysis, the paper concludes with propositions for future work: (1) leveraging the design principles for enhanced concept generation and evaluation through dynamic tradespace exploration and (2) validating the survivability principles beyond the aerospace domain.

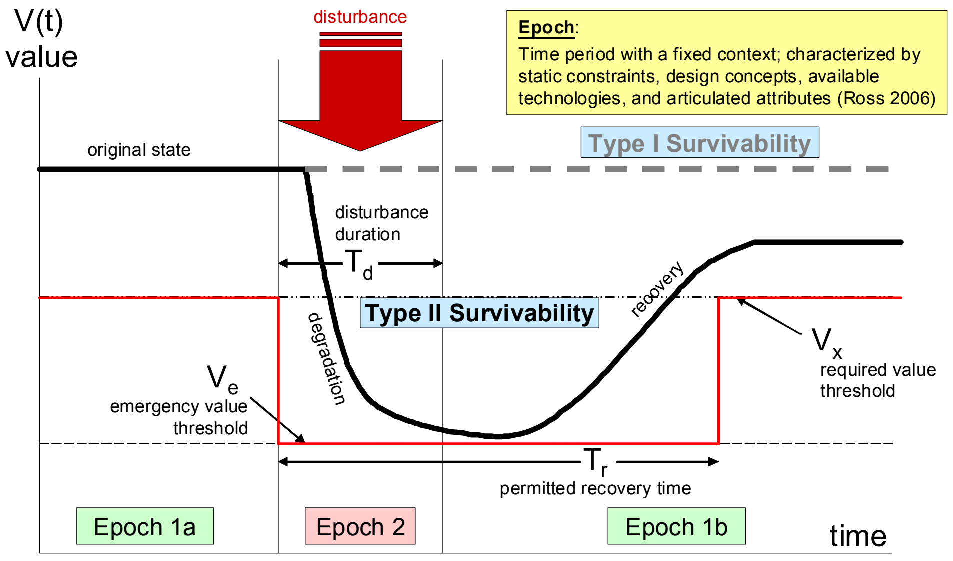

Fig. 1. Definition of Survivability

II. BASELINE SURVIVABILITY DESIGN PRINCIPLES

Survivability is the ability of a system to minimize the impact of a finite-duration disturbance on value delivery [1]. 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. Fig. 1 illustrates Type I and Type II survivability across two epochs, time periods of a fixed context [11]. Type I survivability, appearing as a horizontal grey 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 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 Fig. 1, for example, 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].

Having established a definition of survivability, a generic system-disturbance framework was developed for visualizing and deriving design principles of survivability [12]. 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. For the case of an intelligent adversary, decision-making of the internal and external change agents 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 abstraction of the behavior of the external agent is inspired by the Boyd cycle, also known as the Observe, Orient, Decide, and Act (OODA) loop [13]. (In this research, the orient phase is considered a subset of the decide phase.) The ODA cycle representation of the decision-making of an intelligent adversary was employed to identify the design principles of survivability that are related to the strategic interaction between the internal and external change agents.

Utilizing the generic system-disturbance representation, twelve design principles for enhancing survivability were initially deduced [12]. Subsequent research tested the validity of these results 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 [10]. Results from this mapping identified missing design principles, taxonomic imprecision in design principle definitions, and deficiencies in the underlying system-disturbance framework—informing an expanded set of seventeen design principles (Table 1) that includes a total of seven modifications or additions to the original Type II design principles.

Given the extensive revisions required of the survivability framework and design principle set following the first two empirical tests, it was necessary to conduct more tests. Recognizing that both the A-10 and UH-60 were designed for low vulnerability—and that every design principle

Table 1. Baseline 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

modification involved Type II survivability—it is especially important to explore systems designed for low susceptibility to address validation of the Type I design principles. The following section presents the methodology and the results of two additional empirical tests.

III. EMPIRICAL TESTING

In this section, the validity of the baseline set of seventeen design principles (Table 1) is empirically tested through an inductive mapping of survivability features in existing systems. 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 F-16 combat aircraft and (2) the Iridium space-based telecommunications system.

A. Methodology

The process of empirically testing the survivability design principles begins by attempting to establish traceability from survivability features in operational systems to the seventeen 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 two sections, matrices are used to qualitatively illustrate traceability of survivability features in operational systems to the seventeen design principles. One matrix is constructed for each system under investigation. Survivability features (grouped by subsystem or architectural component) comprise the rows and the seventeen preliminary design principles comprise the columns. Relationships are represented with "X" marks – an indication that one of the functional requirements of the design feature achieves survivability (*i.e.*, positively affects value delivery over the lifecycle of a disturbance) utilizing a particular set of design principles. It is expected that utilization of a particular feature should involve the application of one or more design principles. (An additional column, marked "ODA–exclusive," is reserved for declared survivability features in operational systems which support the achievement of survivability but do not positively affect value delivery in isolation. For example, situational awareness is a prerequisite to the utilization of any survivability feature requiring decision making but, by itself, does not make a system more survivable.) If logical inconsistencies or other issues arise while establishing traceability, those portions of the matrices 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, 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 F-16C combat aircraft and Iridium satellite communications network were selected for the empirical tests. When combined with the A-10A Warthog and UH-60A Blackhawk empirical tests, this sample draws across four major classes of aerospace systems: helicopters, aircraft designed for low-susceptibility, aircraft designed for low-vulnerability, and spacecraft. 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 [4] among a constellation of satellite systems rather individual constituent nodes.

B. Test #1 – F-16C (Block 40) Fighting Falcon

The F-16 "Fighting Falcon" (Fig. 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 [7]. 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 [14, 15].

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 [17]. 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 [14]. 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.

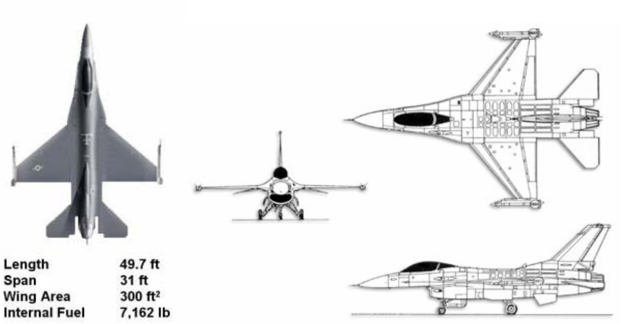

Fig. 2. F-16C Fighting Falcon [16]

To test the baseline set of design principles, survivability features were gathered from open-source literature on the F-16C, Block 40 Build [14–21]. (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 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 2. Tracing F-16 Survivability Features to Design Principles

		Type I (Reduce Susceptibility)						Type II (Reduce Vulnerability)											ODA - exclusive
	F-16C: Sample Survivability Features	prevention	mobility	concealment	deterrence	preemption	avoidance	hardness	redundancy	margin	heterogeneity	distribution	reduction	fail-safe	evolution	containment	replacement	repair	
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.

C. Test #2 – Iridium Communications Network

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 [22]. Iridium employs a unique concept-of-operations for commercial space communications by providing connectivity between satellites using dynamic crosslinks [23]. While its economic failure is worthy of a value-centric analysis [24], Iridium is also an interesting case application for the design principle framework in terms of physical survivability because the communications service is achieved not only by the individual Iridium satellites but also by the overall network architecture. Existing research has evaluated Iridium constellation survivability by comparing packet rejection rates, hop counts, and average end-to-end delay performance of degraded Iridium constellations [25]. This research and related analyses [26] 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

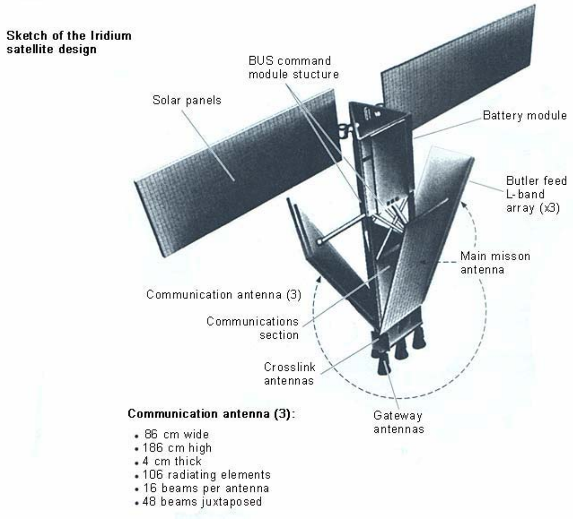

Fig. 3. Iridium Satellite [Iridium LLC]

Table 3. Tracing Iridium Survivability Features to Design Principles

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

milliseconds).

To test the baseline set of design principles, survivability features were gathered on the Iridium architecture from the literature [22-37]. 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 3 presents the results of this empirical mapping. In contrast to the F-16, 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 [22].) These constellation level survivability features include dynamic control and routing of satellite crosslinks around unavailable nodes, on-orbit satellite satellite spares, and the ability to control all 66 operational spacecraft from a single ground facility. "…[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" [22].

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.)

IV. SYNTHESIS

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. In the F-16 and Iridium case applications in the

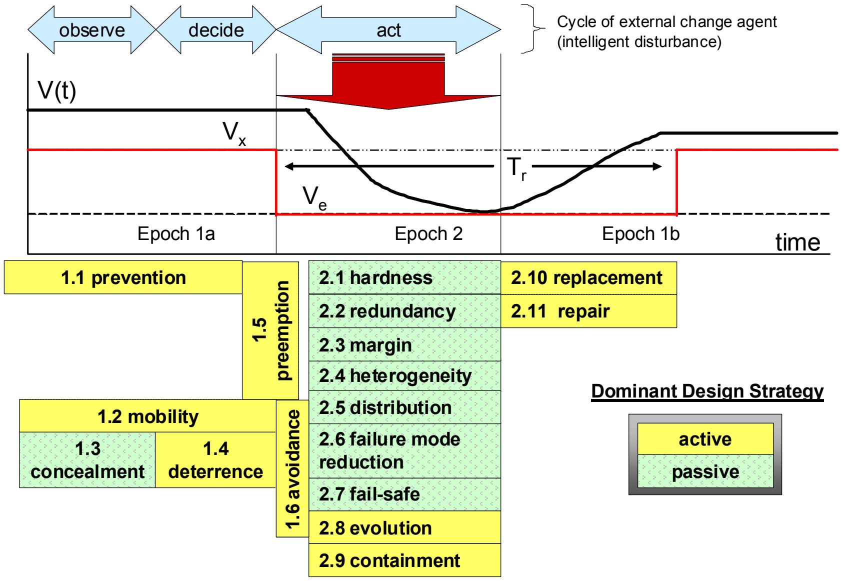

Fig. 4. Temporal Mapping of Design Principles to Disturbance Lifecycle

previous section, the design principle framework was shown to be complete and applicable to the survivability features of two real systems. Taken as a whole with previous empirical test cases (*e.g.*, A-10, UH-60), the completed case applications support the validity of the design principles within the aerospace domain. While all survivability features of the F-16 and Iridium system were successfully mapped to the design principles identified previously, the process of establishing traceability also provided deeper understanding regarding two aspects of the underlying survivability framework: (1) distinction between passive and active survivability and (2) the ODA cycle of the external change agent.

As discussed in previous work [1, 12], the design principles may be broadly decomposed into passive principles that seek to maintain value delivery through static design elements and active principles that focus on either eliminating disturbances or on agile architectures for rapid recovery. Fig. 4 decomposes each of the seventeen principles into one of these two broad groups and illustrates when each positively affects system value delivery during the lifecycle of a disturbance. In the process of mapping certain F-16 survivability features to the design principles—chaff and flare dispensers, defensive jamming, decoying—it was realized that some design principles are not amenable to this binary categorization of passive and active survivability. These F-16 survivability features are active in nature, requiring situational awareness, decision making, and action by the pilot (*i.e.*, the ODA cycle of the internal change agent). A new design principle of "active concealment" (*e.g.*, *suppression*) was considered for addition to the set of Type I design principles. However, this design principle would have been redundant with *concealment*, the reduction of the visibility of a system from an external change agent. Therefore, it was recognized that the passive/active attributes of the design principles are not absolute distinctions but rather representative of a continuum between two different design philosophies.

The second, deeper understanding gained from the two case applications was the importance of the ODA cycle of the external change agent for ensuring full enumeration of survivable concepts. Having completed four empirical tests of the design principles, it was found that survivability features of the systems had never been independently traced to *mobility*, mobility having always been traced with *avoidance*. Given the desire to minimize the number of design principles while maintaining collective exhaustiveness, mobility was considered for elimination as a design principle. However, as defined in Table 1, mobility serves to disrupt the observation phase of the external ODA cycle while avoidance disrupts the action phase. Given that both phases are critical for the external change agent to successfully disrupt the system, each design principle may be employed independently in future systems to achieve survivability.

V. CONCLUSION

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. Based on the results of the experiments in this paper and previous experimentation [10], the seventeen general design principles are found to characterize all of the survivability features employed by 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. Future work will be required to test the applicability of the survivability design principles outside of the aerospace domain (*e.g.*, civil infrastructure, organizational resilience).

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.

ACKNOWLEDGEMENT

The authors gratefully acknowledge support for this research from the MIT Systems Engineering Advancement Research Initiative (http://seari.mit.edu) and the MIT Program on Emerging Technologies (http://poet.mit.edu/).

REFERENCES

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

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

[3] GAO (2002). "Critical Infrastructure: Commercial Satellite Security Should Be More Fully Addressed." Report to U.S. Senate, Government Accounting Office.

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

[5] JTCG/AS (2001). Aerospace Systems Survivability Handbook. Arlington, VA, Joint Technical Coordinating Group on Aircraft Survivability.

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

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

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

[9] R. Jugulum, and D. Frey (2007). "Toward a Taxonomy of Concept Designs for Improved Robustness." *Journal of Engineering Design*, 18(2): 139-156.

[10] M. Richards, A. Ross, D. Hastings and D. Rhodes (2008). "Two Empirical Tests of Design Principles for Survivable System Architecture." SEAri Working Paper 2008-2-1, *http://seari.mit.edu/documents/working_papers/SEAri_WP-2008-2-1.pdf*.

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

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

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

[14] R. Dorr, (1991). "F-16 Fighting Falcon." *World Airpower Journal*, 5(Spring 1991): 50-111.

[15] M. Rosenwald, (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.

[16] See *http://www.aerospaceweb.org/question/planes/q0163.shtml*

[17] E. Hehs, (1999). "F-16 Refresher Course." *Code One: An Airpower Projection Magazine*, April 1999.

[18] F. Ahmed-Zaid, P. Ioannou, K. Gousman and R. Rooney (1991). "Accomodation of Failures in the F-16 Aircraft Using Adaptive Control." *IEEE Control Systems Magazine*, 11(1): 73-78.

[19] ACC (1996). "Multi-Command Handbook on F-16 Combat Aircraft Fundamentals." Air Combat Command (ACC).

[20] J. Blaylock, and D. Swihart (1997). "Application of Advanced Safety Technique to Critical Subsystem Integration." *AIAA Guidance, Navigation, and Control Conference*, New Orleans, LA.

[21] S. Thomas, H. Kwatny, B. Chang and C. Belcastro (2005). "Regulator Design for Control Surface Failure Accomodation in an F-16." *AIAA Guidance, Navigation, and Control Conference*, San Francisco, CA.

[22] T. Garrison, J. Pizzicaroli and P. Swan (1997). "Systems Engineering Trades for the IRIDIUM Constellation." *Journal of Spacecraft and Rockets*, 34(5): 675-680.

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

[24] O. de Weck, 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.

[25] D. Stenger, (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.

[26] C. Fossa, 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.

[27] G. Comparetto, and N. Hulkower (1994). "Global Mobile Communications: A Review of Three Contenders." *AIAA 15th International Communications Satellite Systems Conference*, San Diego, CA.

[28] K. Maine, C. Devieux and P. Swan (1995). "Overview of Iridium Satellite Network." *Wescon Application Conference*, San Francisco, CA.

[29] J. Pizzicaroli, (1997). "Launching and Building the IRIDIUM Constellation." *Mission Design and Implementation of Satellite Constellations*, Toulouse, France.

[30] P. Swan, (1997). "A Revolution in Progress: IRIDIUM LEO Operations." *AIAA Defense and Space Programs Conference*, Huntsville, AL.

[31] J. Karpiscak, (1998). "Proliferation of Commercial Space Systems - Benefits and Concerns for U.S. Combat Operations." *AIAA Defense and Civil Space Programs Conference*, Huntsville, AL.

[32] P. Lemme, S. Glenister and A. Miller (1998). "Iridium Aeronautical Satellite Communications." *Digital Avionics Systems Conference*, Belleview, WA.

[33] S. Pratt, 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.

[34] A. Puderbaugh, 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.

[35] M. Iovanov, 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.

[36] G. Swinerd, 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.

[37] Y. He, and H. Zhao (2007). "Survivability Performance Evaluation for Satellite Communication Network Based on Walker Constellation." *SPIE Conference on Space Information Technology*, Wuhan, China.