DESIGN PRINCIPLES FOR SURVIVABLE SYSTEM ARCHITECTURE

Matthew G. Richards
mgr@mit.edu

Adam M. Ross
adamross@mit.edu

Daniel E. Hastings
hastings@mit.edu

Donna H. Rhodes
rhodes@mit.edu

Massachusetts Institute of Technology
77 Massachusetts Ave., NE20-343
Cambridge, MA 02139

Abstract - A key challenge confronting system architects is the specification, development, procurement, operation, and maintenance of systems with critical survivability requirements. To address this challenge, a generic framework for analyzing system interactions with natural and synthetic hostile environments is introduced and twelve design principles are proposed for the achievement of survivable system architecture.

INTRODUCTION

Survivability is traditionally defined in military systems as the capability to avoid or withstand a hostile environment. For example, Ball (2003) analyzes design techniques, armaments, and tactics for combat aircraft survivability [1]. In Ball's framework, survivability is enhanced by both reductions in the susceptibility of systems to disturbances (*e.g.*, stealth, maneuverability) and reductions in the vulnerability of systems to disturbances (*e.g.,* redundant flight controls and surfaces, independent fuel feed tanks).

In this paper, survivability is defined as the ability of a system to minimize the impact of a finite disturbance on value delivery [2]. Similar to Ball's formulation, a two-part definition of survivability is developed in terms of reducing susceptibility and reducing vulnerability. In particular, it is found that 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). The primary goal of this paper is to enumerate design principles for the achievement of both Type I and Type II survivability.

The body of the paper consists of four sections. First, motivation is provided for research on survivable architecture as a pathway to value-robust engineering systems. This includes a review of the literature as well as a retrospective look at a "flagship" example of survivable architecture—the Cold War-era U.S. nuclear command and control system. Second, a preliminary framework is introduced for modeling survivability as the interaction between a system and a given hostile environment. The framework includes a formal definition of survivability and a simple network representation of system architecture and its associated context.

After providing a descriptive framework, the third section proposes twelve design principles for enhancing survivability. In particular, six design principles for enhancing Type I survivability are 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 are also enumerated: (2.1) hardness, (2.2) evolution, (2.3) redundancy, (2.4) diversity, (2.5) replacement, and (2.6) repair. In the fourth section, the temporal properties of these twelve design principles are mapped to a disturbance lifecycle. The paper concludes with a discussion of the implications of the framework and challenges associated with architecting survivable systems.

MOTIVATION

The operational environment of engineering systems is increasingly characterized by disturbances which 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 [3], the Northeast Blackout of 2003 [4], and Hurricane Katrina [5]. More recently, China's successful test of an anti-satellite (Asat) weapon against an aging Chinese Feng Yun 1C weather satellite on January 11, 2007, has incited calls for enhancing spacecraft survivability [6]. 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 [7].

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 [8]. 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 [9]. Although survivability is an emergent property of system architecture that has meaning primarily in the overall context to which it relates, conventional approaches to survivability engineering are often reductionist in nature (*i.e.*, focused only on selected properties of certain subsystems or modules in isolation). Furthermore, existing survivability engineering methodologies are based on domain-specific operating scenarios and presupposed disturbance environments and provide limited insights for senior decision-makers trading system survivability for cost and utility at the highest levels in the system architecture. Development of a generic survivability framework and associated design methodologies represents both a need and an opportunity for growth within systems architecting.

Lessons Learned from U.S. Nuclear Command and Control System

Before providing prescriptive statements regarding survivable system architecture, it is necessary to understand existing principles, methods, and tools. While a survey of the existing design paradigms for survivability is outside of the scope of this paper, a descriptive look at existing survivable architectures is necessary for establishing a baseline for enumerating design principles. In this spirit, a retrospective overview of a "flagship" example of survivable system architecture is provided—the U.S. Nuclear Command and Control System (NCCS) during the Cold War.

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

Rather than analyzing all military systems associated with strategic deterrence, the focus here is on the NCCS. When the U.S. switched from a policy of massive retaliation to one of flexible response in 1961, survivable communications

(*i.e.*, maintaining operational capability after a Soviet first-strike) between central authorities and the nuclear forces became a military requirement.[1] As a system designed against this nuclear decapitation attack scenario, the NCCS is a strong candidate for a case study on survivability.

The NCCS may be functionally decomposed into five areas: situation monitoring, tactical warning, decision-making, force management, and force direction [10]. Situation monitoring includes both the collection of strategic intelligence to anticipate crises and weather monitoring to support airborne operations. Tactical warning consists of the set of activities to determine the origin, size, and target of an attack. In supporting decision-makers in crafting a response, tactical warning requires a high degree of certainty (*e.g.*, dual phenomenology provided by satellites and radars). Force management and direction includes the standard operating procedures involved in assuring negative and positive control (*i.e.*, prevention of accidental launches and implementation of presidential release orders, respectively).

The current survivability of the NCCS is attributed to four design principles: (1) hardening, (2) mobility, (3) redundancy, and (4) concealment [10]. These four design principles manifest themselves differently in the various nodes and links of the NCCS (*e.g.*, contrast hardening of the NORAD Cheyenne Mountain Complex to the Milstar satellite constellation). Additionally, each design principle does not contribute equally to architecture survivability. For example, in the early 1980's, there were concerns that Soviet strategic forces could overwhelm virtually all U.S. ground-based command and control and that the U.S. was dependent on airborne command posts and TACAMO relay aircraft for post-attack control over the submarine force [11,12]. These concerns suggest that mobility was more important for achieving NCCS survivability than the hardening and redundancy provided by the network of fixed command locations in the Pentagon, Offutt Air Force Base, Fort Ritchie, and Cheyenne Mountain [10].

[1] If early warning sensors detected a nuclear attack by the Soviet Union during the period of 1955-60, U.S. policy was to launch a full retaliation between the time of launch and strike. As such, the NCCS was superfluous after the Presidential release order and was therefore not originally designed for survivability [11].

While the four design principles of NCCS survivability discussed above provide a fairly complete enumeration of the physical attributes providing survivability, the discussion neglects critical architectural elements of operational behavior and organizational design. For example, with decision cycles in a nuclear war measured in minutes [12], development of a scripted operational plan for every conceivable contingency may be as essential to providing a credible deterrent against a decapitation threat as the survivability of the nuclear force itself.

The sensitivity of NCCS survivability to operational behavior and organizational design is best illustrated in the transition in the 1960's away from the massive retaliation policy to a flexible response paradigm that required NCCS survivability [11]. Facing the challenge of inheriting a legacy NCCS infrastructure that was not designed for survivability but without resources to build a new infrastructure, designers succeeded in re-architecting the existing NCCS infrastructure for survivability by restructuring tactics, procedures, and operating rules. In particular, the decapitation risk was mitigated by making the presidential command center a "safety catch" that, when operational, prevented other command centers from firing. If the safety catch was removed, second-strike emergency authorization is implicitly granted to decentralized authorities (*i.e.*, one- and two-star generals), removing the prospect of a single-point failure in the command structure.

Four main lessons may be extracted from tracing the evolution of NCCS through the Cold War with implications for survivable system architecture. First, the success in re-architecting the system for survivability in the 1960's illustrates the importance of considering methods that extend beyond the domain of physical design to include organizations and operational behavior. Given the success in transitioning the NCCS in the 1960's from a non-survivable to a survivable architecture without major physical modifications, might it be possible similarly to transition critical U.S. infrastructures to less vulnerable states today by restructuring procedures and operating rules? Second, the emphasis on executing scripted contingency plans underscores the criticality of timely decision-making under uncertainty within hostile environments. Third, the strategic interactions characterizing the NCCS context (*e.g.*, Mutually Assured Destruction) suggests that it is not adequate to consider individual disturbance events when dealing with an intelligent adversary.

Rather, it is necessary to take a longer view by considering design principles for lifecycle survivability which may influence the strategic behavior of adversaries. Fourth, while the NCCS is an excellent case for enumerating design principles for survivability, it is important to note its limitations: (1) the design principles explicitly linked to NCCS survivability [10] are limited to the physical domain, and (2) the design principles as manifested in the NCCS are not economically deployable to current survivability challenges such as those associated with hardening critical public infrastructures. Accordingly, two of the goals of this research are to provide a complete enumeration of design principles for survivability and to develop a methodology for parsing out the required principles for a given design.

THEORETICAL FRAMEWORK

After providing a value-centric definition of survivability, this section introduces a preliminary framework for modeling survivability as the outcome of the interaction between a system and a given hostile environment.

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 (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 [13]. This is particularly useful for considering survivability issues when original value delivery mechanisms may be blocked due to 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 [2].

> *Survivability is the ability of a system to minimize the impact of a finite disturbance on value delivery.*

As noted in Ball's formulation for aircraft combat survivability [1], 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 survivability across two epochs [13], time periods of a fixed environment. 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 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 expected value threshold [V_x] within the permitted recovery time [T_r]. Type I survivability would have been achieved if the disturbance never reduces the delivered value [V(t)] below the expected value threshold [V_x] and would appear to be a relatively straight line in a similar figure.

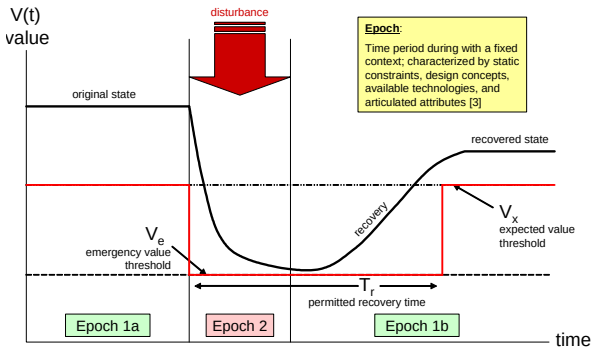

Figure 1. Type II Survivability

Having established a definition of survivability, a preliminary framework is developed for visualizing the 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 (1) a simple network representation of heterogeneous nodes and arcs of the technical system architecture, (2) a system operator characterized by an internal change agent, and (3) a hostile environment characterized by an external change agent. Changes in the arrangement of these three elements will be used to provide insights into survivability.

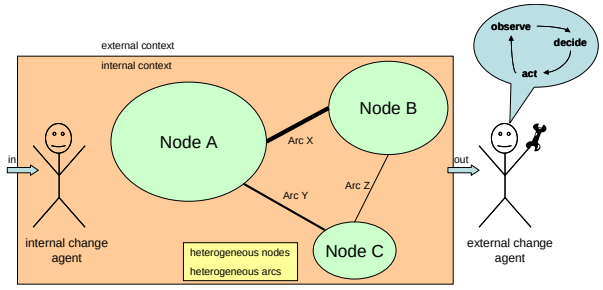

Figure 2. Survivability Framework

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 [14]. 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 is used in this paper to parse out the design principles of survivability that are related to the strategic interaction between the internal and external change agents.

PROPOSED DESIGN PRINCIPLES

Utilizing the framework developed above, this section enumerates twelve design principles of survivability. These are classified as six design principles for Type I survivability and six design principles for Type II survivability.

Type I Survivability

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

Prevention (1.1)

Prevention is *the suppression of a future or potential future disturbance*. Through the prevention design principle, disturbances are not given the opportunity to become a threat to the system. Examples of the principle include aircraft suppression of enemy air defense (SEAD) before a conflict, intended to remove threats to friendly aircraft, and the instigation of the second Persian Gulf War, intended to prevent the Iraq regime from developing weapons of mass destruction.

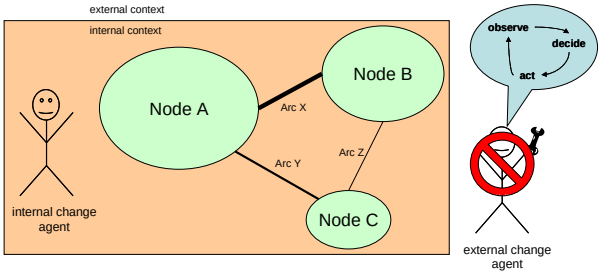

Figure 3. Prevention

Mobility (1.2)

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

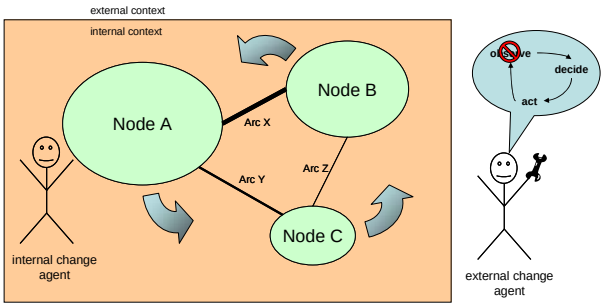

Figure 4. Mobility

Concealment (1.3)

Concealment is *the act of reducing the visibility of a system from an external change agent*. Through the concealment design principle, the disturbance agent's ability to effectively observe the system is diminished because the system is difficult to identify or isolate, thereby making a decision to attack the system more difficult. Examples of the principle include the B-2 Spirit stealth bomber and the F-117 Nighthawk stealth aircraft.

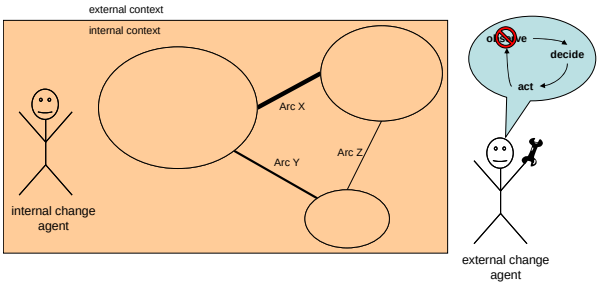

Figure 5. Concealment

Deterrence (1.4)

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

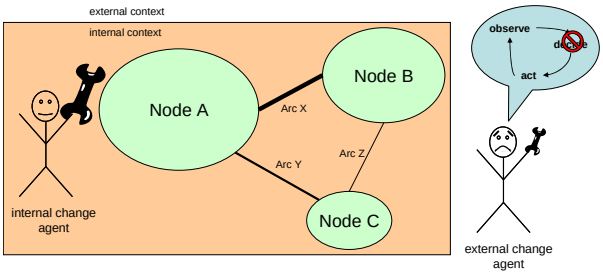

Figure 6. Deterrence

Preemption (1.5)

Preemption is *the suppression of an imminent disturbance*. Through the preemption design principle, the disturbance agent's ability to act is removed or diminished immediately prior to committing the act. Examples of the principle include missile defense and the Israeli attack on Egyptian forces in the 1967 Six Day War.

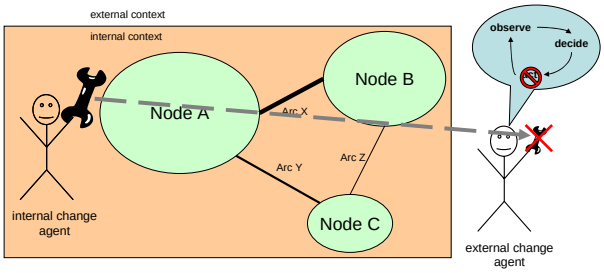

Figure 7. Preemption

Avoidance (1.6)

Avoidance is *the ability to maneuver away from a disturbance*. Through the avoidance design principle, the disturbance agent's action is reduced in effectiveness through the system actively relocating. Examples include aircraft missile evasion and precision landing technology on Mars Science Laboratory (MSL).

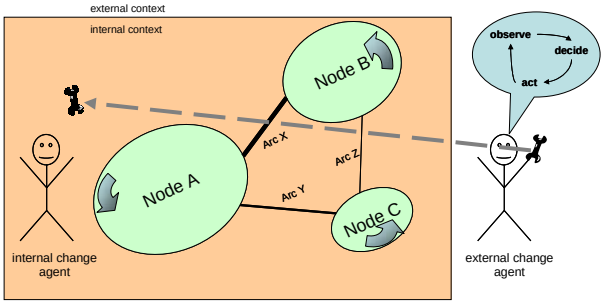

Figure 8. Avoidance

Type II Survivability

The six principles for enhancing Type II survivability (*i.e.*, reducing vulnerability) are: (2.1) hardness, (2.2) evolution, (2.3) redundancy, (2.4) diversity, (2.5) replacement, and (2.6) repair.

Hardness (2.1)

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

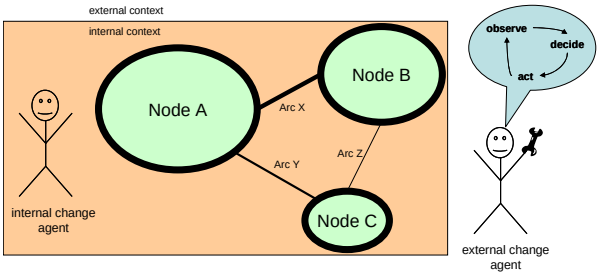

Figure 9. Hardness

Evolution (2.2)

Evolution is *the alteration of system elements to reduce disturbance effectiveness (engineered mismatch)*. Through the evolution design principle, the system actively changes itself to reduce the effectiveness of a disturbance. Examples include the addition of early warning sensors to strategic deterrence missions and dynamically reconfigurable networks.

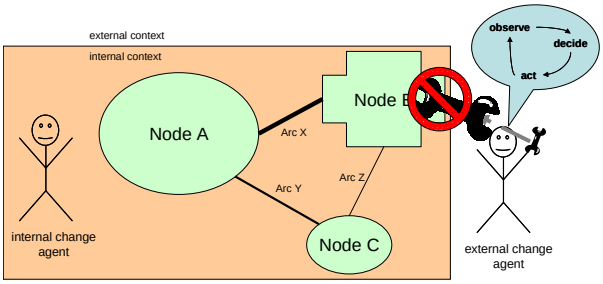

Figure 10. Evolution

Redundancy (2.3)

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

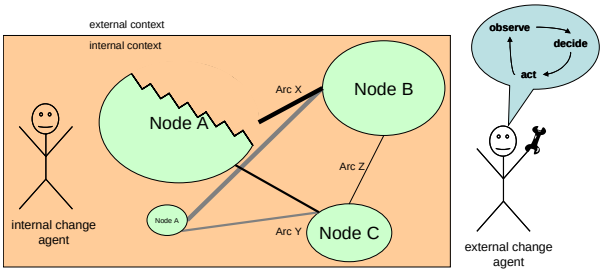

Figure 11. Redundancy

Diversity (2.4)

Diversity is *having variation in system elements (characteristic or spatial) to decrease effectiveness of homogeneous disturbances*. Through the diversity principle, the system reduces the likelihood of the disturbance being able to affect components. Examples include heterogeneous operating systems decreasing the effectiveness of malware, distributed computer networks, and the nuclear "triad."

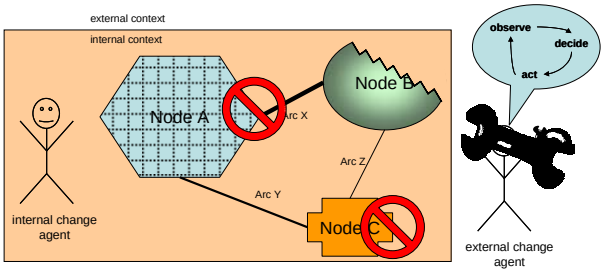

Figure 12. Diversity

Replacement (2.5)

Replacement is *the substitution of system elements to improve value delivery*. Through the replacement principle, the system is restored through the substitution of an undamaged element for a damaged component. An example is the launch of XM-3 and XM-4 satellite radio satellites to replace XM-1 and XM-2 due to solar panel fogging that reduced Boeing 702 lifetimes from 15 to 6 years.

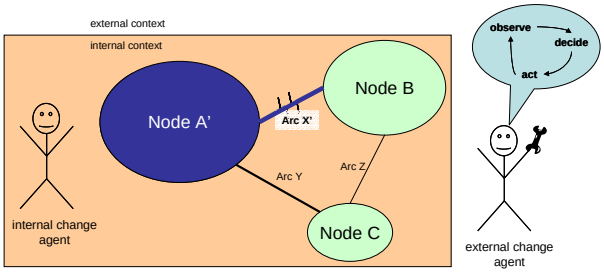

Figure 13. Replacement

Repair (2.6)

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

Replacement (COSTAR) on the Hubble Space Telescope in 1993.

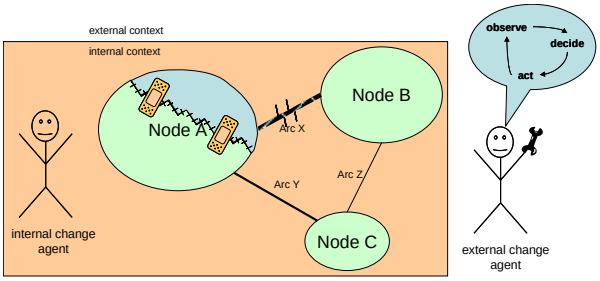

Figure 14. Repair

DESIGN PRINCIPLES AT WORK

This section shows how the twelve design principles map to the disturbance lifecycle (Figure 1). Additionally, a distinction is drawn between passive and active survivability in a discussion on the deployment of the principles by system designers.

Figure 15 depicts the time intervals during which each of the twelve design principles may positively affect value delivery during a disturbance lifecycle. Principles enhancing Type I survivability add value before or during Epoch 2 while Type II principles add value during or after Epoch 2.

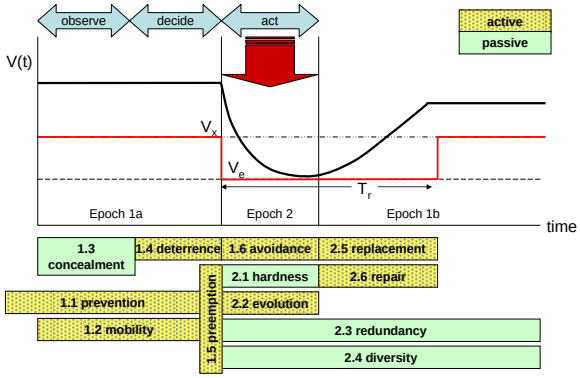

Figure 15. Mapping of Design Principles to Disturbance Lifecycle

Each design principle in Figure 15 is classified as either passive or active. A focus on passive principles will lead to the construction of closed (static) systems that resist disturbance based on projections of the operational environment. A focus on active principles will lead to the construction of open (dynamic) systems that cope with future uncertainty by stressing architectural agility to recover from disturbances (Table 1). The distinction between passive and active survivability is useful because it specifies which design principles may be used based on the changeability [13] of the architecture. For example, the current generation of communications satellites has a low degree of changeability due to the inaccessibility of the orbiting vehicles following launch. In order to achieve survivability in the harsh environment of space, designers focus on the passive design principles of radiation hardening and redundancy (increasing mass, complexity, and cost). If on-orbit servicing vehicles were to be developed, the changeability of communications satellites would increase. This would provide designers the option of incorporating design principles of active survivability such as repair, replacement, and evolution via servicing missions in lieu of costly hardening and radiation techniques [15].

Table 1. Passive vs. Active Survivability

	Passive Survivability	Active Survivability
Philosophy	Survivability is something that a system *has*	Survivability is something that a system *does*
Characteristics	proactive, resistant, robust	reactive, flexible, adaptive
Design Principles	concealment, hardness, redundancy, diversity	prevention, mobility, deterrence, preemption, avoidance, evolution, replacement, repair
Forecasting	Presupposes knowledge of disturbance environment	Acknowledges uncertainty in projection of future disturbances
Architecture	Closed (static)	Open (dynamic)
Design Focus	Defensive barriers at system-level to resist disturbances	Architectural agility to avoid, deter, and recover from disturbances
Failures	Causal chain (often linear)	Tight couplings, functional resonance (nonlinear)
Relevant Disciplines	Component reliability, safety engineering, risk analysis, domain-specific technologies	Real options, organizational theory, process design, domain-specific technologies

The distinction between passive and active survivability is only a first step towards a systems architecting methodology for managing survivability requirements. While the enumeration of design principles is helpful for understanding a larger set of survivability techniques, it is not intended as a systems engineering checklist or requirements specification. Rather, the enumeration provides designers with a portfolio of options from which to consider a larger tradespace of survivable designs. The success of this portfolio of survivable design principles will vary with context. Designs that achieve a successful balance of survivability, performance, and cost will almost certainty incorporate a subset of the twelve principles with varying weights.

CONCLUSION

Given challenges in the specification, development, procurement, operation, and maintenance of systems with critical survivability requirements, twelve design principles for survivability have been enumerated. Survivability was defined in

terms of value and described as emerging from the interaction between a system and its context. As such, each design principle was illustrated as a modification of the interaction between a system and a hostile disturbance agent. Examples of each design principle were provided from existing systems and the temporal impact of each was characterized. In addition, the twelve design principles were classified in terms of both Type I and Type II survivability and in terms of passive and active survivability.

This paper is based on on-going doctoral research on how survivability should be quantified and used as a decision metric in exploring tradespaces during conceptual design. The following five expected research contributions—motivated by recommendations for future work in an ARL report on survivability [8]—provide direction for future research activities.

1. Generic mission models that can be readily tailored to specific systems to evaluate the adequacy of survivability requirements.
2. Fundamental requirements of survivability that can be directly applied to system developments and procurements.
3. Families of systems and network topologies that are inherently robust to catastrophic failures.
4. Systems architectures that enable survivable systems to be built out of less survivable components (generalized dependence).
5. Policy prescriptions for improved acquisitions paradigm.

Next steps include (1) the development of quantitative metrics for each design principle, (2) expert interviews, and (3) incorporation of survivability as an attribute in an existing satellite tradespace. Moving ahead, it is hoped that the design principles proposed in this paper serve as a foundation for future research on survivable system architecture.

REFERENCES

[1] Ball, R., The Fundamental of Aircraft Combat Survivability Analysis and Design, 2nd Edition. Reston: AIAA Education Series, 2003.

[2] Richards, M., Hastings, D., Rhodes, D., and Weigel, A., "Defining Survivability for Engineering Systems." *Conference on Systems Engineering Research*, Hoboken, NJ, March 2007.

[3] Kean, T., Hamilton, L., et al., *National Commission on Terrorist Attacks Upon the United States*. Government Printing Office, 2004.

[4] U.S.-Canada Power System Outage Task Force, *Final Report on the August 14th Blackout in the United States and Canada*, April 2004.

[5] Knabb, R., Rhome, J., and Brown, D., *Tropical Cyclone Report: Hurricane Katrina*. National Hurricane Center, December 2005.

[6] Covault, C., "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.

[7] Rumsfeld, D., et al., *Commission to Assess U.S. National Security Space Management and Organization*. September 2001.

[8] Neumann, P., *Practical Architectures for Survivable Systems and Networks*. SRI International for U.S. Army Research Laboratory, June 2000.

[9] Hollnagel, E., Woods, D., Levenson, N., et al., Resilience Engineering. Hampshire: Ashgate, 2006.

[10] Critchlow, R., *Nuclear Command and Control: Current Programs and Issues*. Congressional Research Service, May 2006.

[11] Bracken, P., The Command and Control of Nuclear Forces. New Haven: Yale University Press, 1983.

[12] Blair, B., Strategic Command and Control: Redefining the Nuclear Threat. Washington DC: The Brookings Institution, 2005.

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

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

[15] Richards, M., *On-Orbit Serviceability of Space System Architectures*. Department of Aeronautics and Astronautics and Engineering Systems Division, dual Master's thesis. Massachusetts Institute of Technology, Cambridge, MA, 2006.