Empirical Validation of Design Principles for Survivable System Architecture

2008 IEEE Systems Conference

Matthew G. Richards
Research Assistant, Engineering Systems Division
Massachusetts Institute of Technology

Adam M. Ross, Ph.D.
Research Scientist, Engineering Systems Division
Massachusetts Institute of Technology

Daniel E. Hastings, Ph.D.
Professor, Aeronautics and Astronautics & Engineering Systems
Massachusetts Institute of Technology

Donna H. Rhodes, Ph.D.
Senior Lecturer, Engineering Systems Division
Massachusetts Institute of Technology

Agenda

- Definition of Survivability
- Motivation for Survivability Design Principles
- Empirical Testing
  - Methodology
  - Baseline Survivability Design Principles
  - Test #1 – F-16 Fighting Falcon
  - Test #2 – Iridium Telecommunications Network
  - Results
- Conclusion

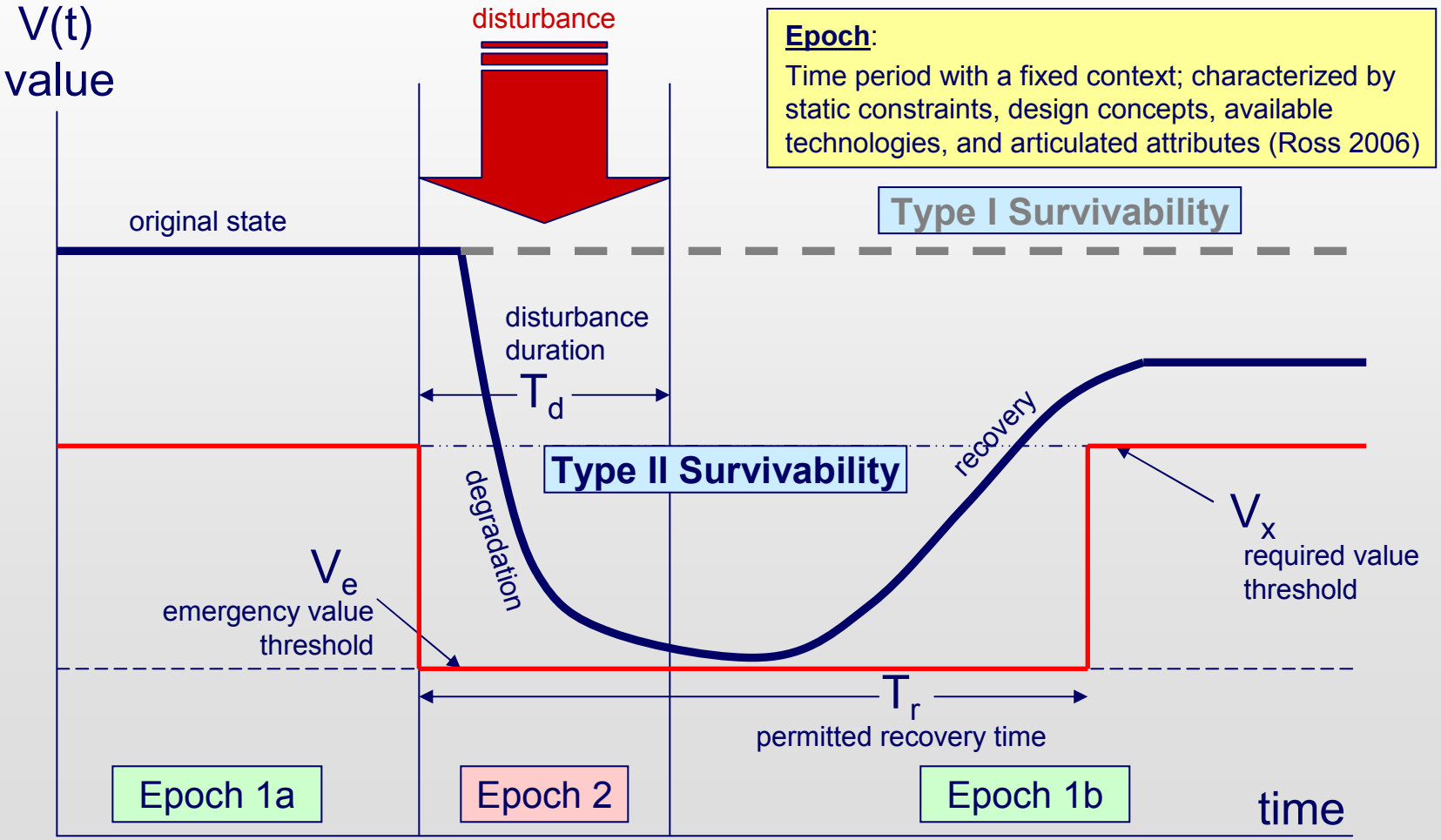
Definition of Survivability

Definitions of Survivability

Domain	Definition / Criteria	Source
Biology	Environmental fitness of organisms; evolutionary longevity of species to natural selection	Darwin 1859
Communication Networks	Percentage of stations both surviving the physical attack and remaining in electrical connection with the largest single group of surviving stations	Baran 1964
	Probability of retaining connection between representative pairs of nodes	Al-Noman 1998
	Ability of a system to perform required functions at a given instant in time after a subset of components become unavailable	Yurcik and Doss 2002
Aerospace / Defense	Quantified ability of a system, subsystem, equipment, process, or procedure to continue to function during and after a natural or man-made disturbance	MIL-STD-188
	Capability of a system and crew to avoid or withstand a man-made hostile environment without suffering an abortive impairment of its ability to accomplish its designated mission	Naval Air Warfare Center 2001

Definition of Survivability

Ability of a system to minimize the impact of a finite-duration disturbance on value delivery through either (I) the reduction of the likelihood or magnitude of a disturbance or (II) the satisfaction of a minimally acceptable level of value delivery during and after a finite disturbance



Epoch:
Time period with a fixed context; characterized by static constraints, design concepts, available technologies, and articulated attributes (Ross 2006)

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


SEA RI
Systems Engineering Advancement Research Initiative

Motivation

Introduction

- Despite increased geographic distribution, information technology has increased ***interdependence*** of systems
- Interdependencies magnify risk from local disturbances that rapidly ***propagate***
- Risks exacerbated by emergence of ***new sources of disturbances***
  - Physical: terrorism
  - Electronic: cyber-attacks
- Shortcomings associated with ***reductionist conventional approaches*** to survivability engineering
  - Limited to physical domain
  - Presuppose operating environments and hazards
  - Ineffective for managing emergent, context-dependent system properties

Research needed on how survivability should inform design decisions of system architectures

Recent Events

Operational environment of engineering systems characterized by increasing number of disturbances

2000
ILOVEYOU internet virus
$10 billion business damage

8/14/2003
Generator in Parma, OH, goes offline
Affected 40 million people in 8 states
$6 billion in losses

1999 — 2006

9/11/2001
3000 lives lost from attacks on WTC and Pentagon
Closed NYSE and NASDAQ until 9/17
US stocks lost $1.2 trillion in value the following week

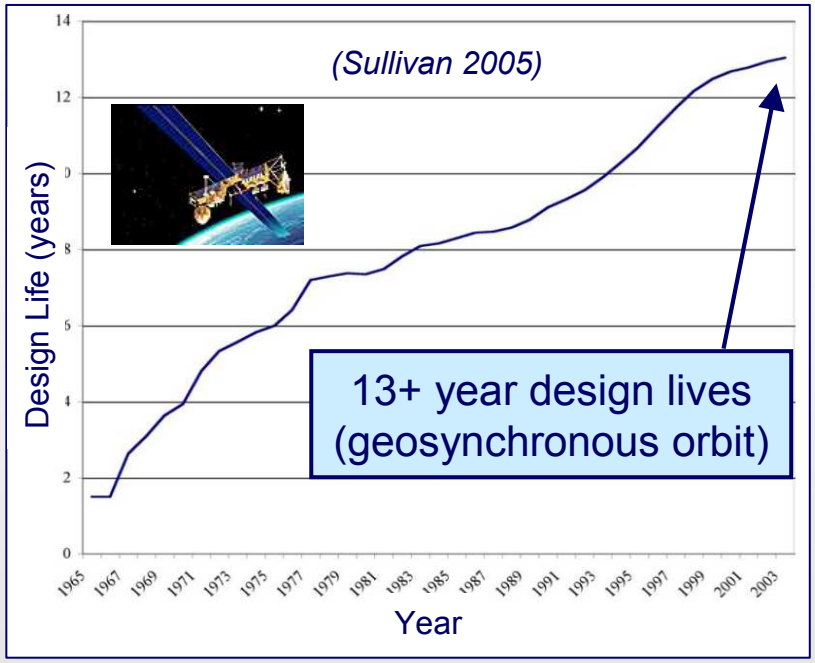
8/28/2005
Hurricane Katrina strikes New Orleans
2000 lives lost
$81.2 billion in damage

Motivation Survivability Challenge in Space Architecture

1960's Paradigm

- CORONA: 30-45 day missions
- 144 spacecraft launched between 1959-1972 *(Wheelon 1997)*

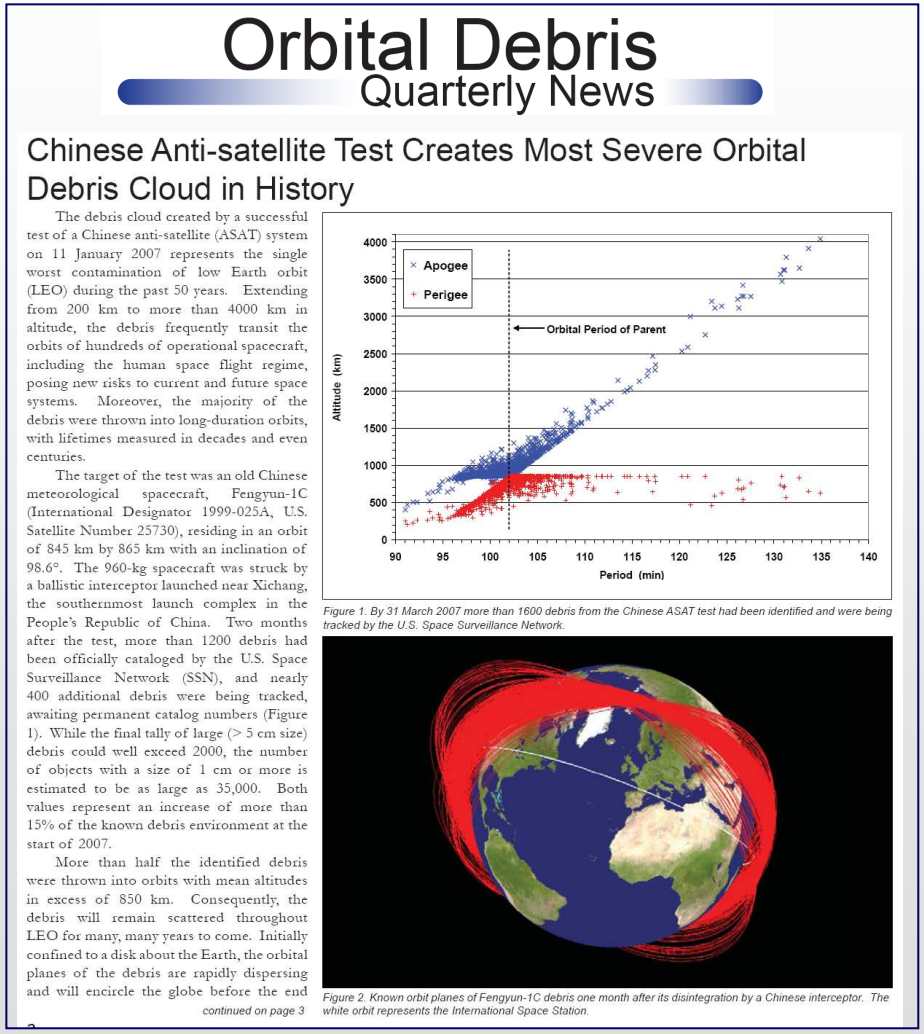
Evolution to Current State



- ***Inability to adapt to uncertain future environments, including disturbances***

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

Satellite Survivability Concerns Exacerbated by Four Trends



Orbital Debris
Quarterly News

Chinese Anti-satellite Test Creates Most Severe Orbital Debris Cloud in History

The debris cloud created by a successful test of a Chinese anti-satellite (ASAT) system on 11 January 2007 represents the single worst contamination of low Earth orbit (LEO) during the past 50 years. Extending from 200 km to more than 4000 km in altitude, the debris frequently transit the orbits of hundreds of operational spacecraft, including the human space flight regime, posing new risks to current and future space systems. Moreover, the majority of the debris were thrown into long-duration orbits, with lifetimes measured in decades and even centuries.

The target of the test was an old Chinese meteorological spacecraft, Fengyun-1C (International Designator 1999-025A, U.S. Satellite Number 25730), residing in an orbit of 845 km by 865 km with an inclination of 98.6°. The 960-kg spacecraft was struck by a ballistic interceptor launched near Xichang, the southernmost launch complex in the People's Republic of China. Two months after the test, more than 1200 debris had been officially cataloged by the U.S. Space Surveillance Network (SSN), and nearly 400 additional debris were being tracked, awaiting permanent catalog numbers (Figure 1). While the final tally of large (> 5 cm size) debris could well exceed 2000, the number of objects with a size of 1 cm or more is estimated to be as large as 35,000. Both values represent an increase of more than 15% of the known debris environment at the start of 2007.

More than half the identified debris were thrown into orbits with mean altitudes in excess of 850 km. Consequently, the debris will remain scattered throughout LEO for many, many years to come. Initially confined to a disk about the Earth, the orbital planes of the debris are rapidly dispersing and will encircle the globe before the end

continued on page 3

Figure 1. By 31 March 2007 more than 1600 debris from the Chinese ASAT test had been identified and were being tracked by the U.S. Space Surveillance Network.

Figure 2. Known orbit planes of Fengyun-1C debris one month after its disintegration by a Chinese interceptor. The white orbit represents the International Space Station.

1. Growth of military and commercial dependency on space systems

   (Gonzales 1999; GAO 2002; Ballhaus 2005)

2. Identified vulnerabilities in the U.S. space architecture

   (Thomson 1995; Rumsfeld, Andrews et al. 2001; CRS 2004)

3. Proliferation of threats

   (Rumsfeld, Andrews et al. 2001; Joseph 2006)

4. Weakening of the sanctuary view in military space policy

   (Mowthorpe 2002; O'Hanlon 2004; Covault 2007)

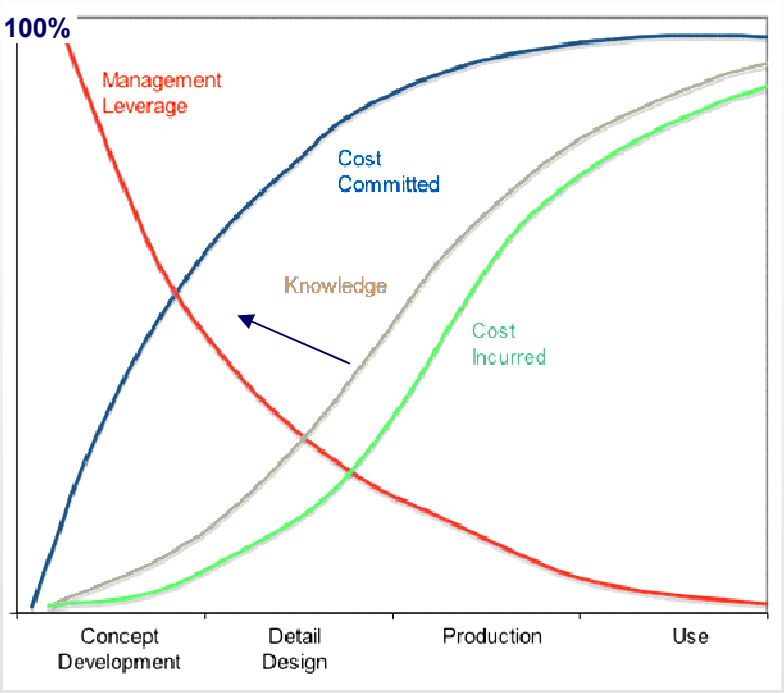
Research Questions

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

Motivation: Improve Concept Generation

- Concept development activities:
  - Identification of stakeholders
  - Enumeration and evaluation of design alternatives
  - Selection of one or more concepts for further development
- Variety of methods for evaluating survivability
- Few methods for generation of alternatives
  - Domain-specificity
  - Emphasis on physical attributes
  - Focus on individual system, not overall architecture delivering end-user value

Critical front-end in complex system design



(Gruhl 1992; Blanchard and Fabrycky 2006)

Related Work

- Survivability enhancement concepts for combat aircraft

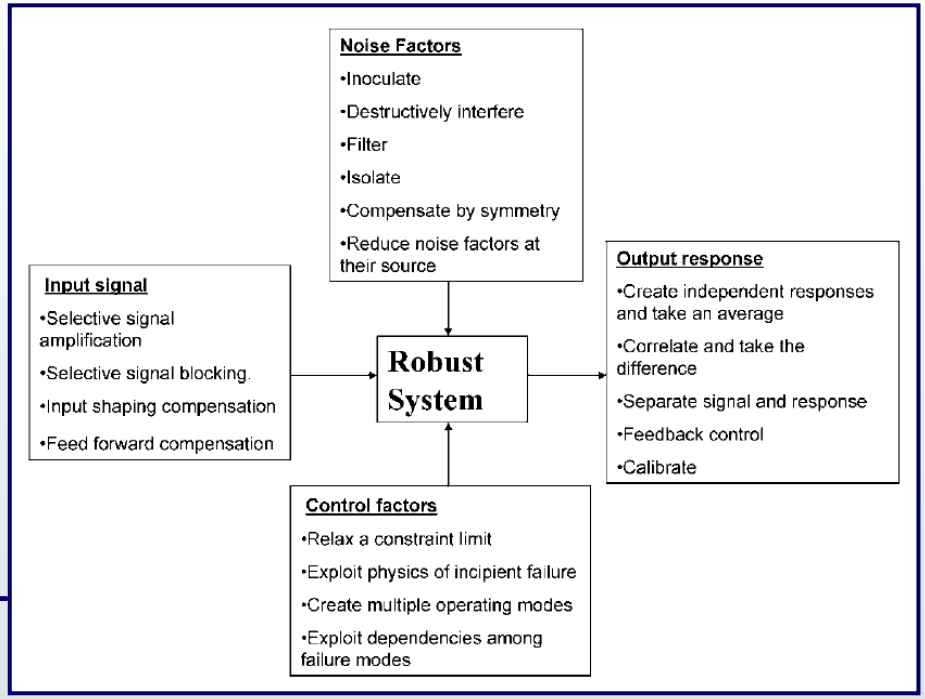
  (Ball 2003)

- Application of survivability principles from biological systems to design of networked services

  (Nakano and Suda 2007)

- Extraction of robust design strategies from U.S. patent database

  (Jugulum and Frey 2007)



Need ***generic*** framework for systematic generation of system concepts that positively affect value delivery over the lifecycle of a disturbance

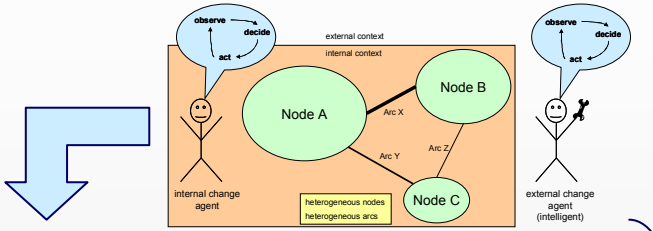
Empirical Testing

Four-Step Methodology (1/4)

Systems Engineering Advancement Research Initiative

Methodology

1. Deduce design principles from generic system-disturbance representation



Type I Survivability (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

literature

interviews

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

Four-Step Methodology (2/4)

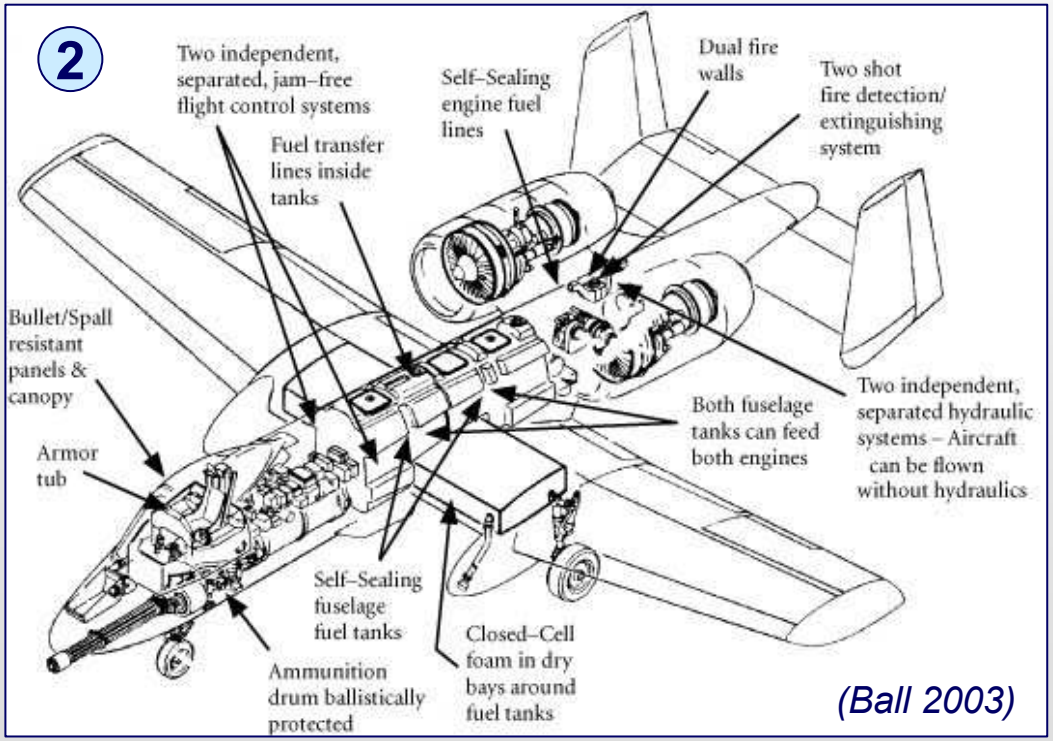
Methodology

1. Deduce design principles from generic system-disturbance representation
2. **Select operational systems with survivability requirements**

①

	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

②



(Ball 2003)

A-10A "Warthog"

Design emphasis on vulnerability

"Airborne tank" aka "Titanium Bathtub" response to effective low level anti-aircraft gunfire during Vietnam

Source: 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.

Four-Step Methodology (3/4)

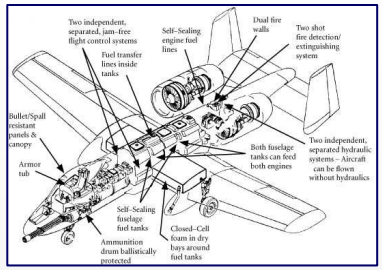
Methodology

1. Deduce design principles from generic system-disturbance representation
2. Select operational systems with survivability requirements
3. **Trace design specifications to design principles**

(1)

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

(2)



(3)

A-10 "Warthog"

Sample Survivability Features

		Type I (Reduce Susceptibility)						Type II (Reduce Vulnerability)					
		prevention	mobility	concealment	deterrence	preemption	avoidance	hardness	evolution	redundancy	diversity	replacement	repair
structure	redundant primary structure									X			
	dual vertical stabilzers 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			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					

margin

Source: 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.

Four-Step Methodology (4/4)

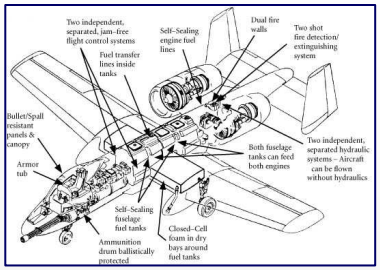
Methodology

1. Deduce design principles from generic system-disturbance representation
2. Select operational systems with survivability requirements
3. Trace design specifications to design principles
4. **Revise design principle set to reflect empirical observation**

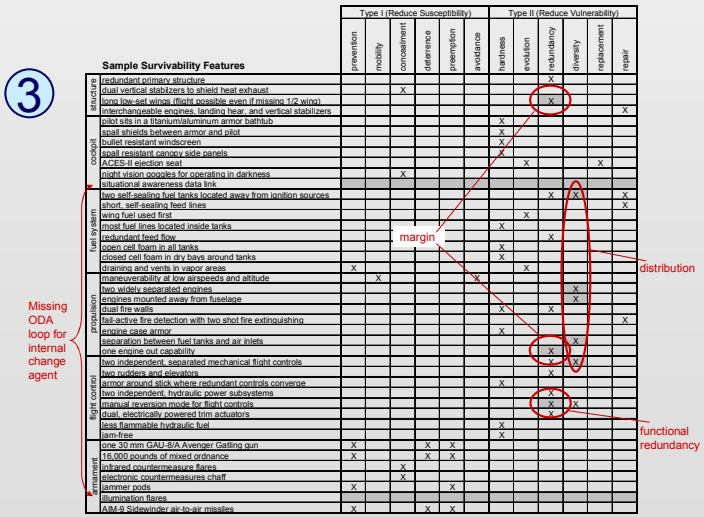
1

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

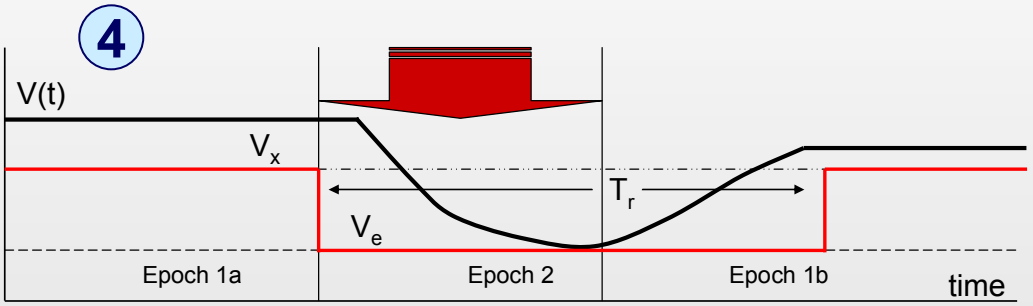
2

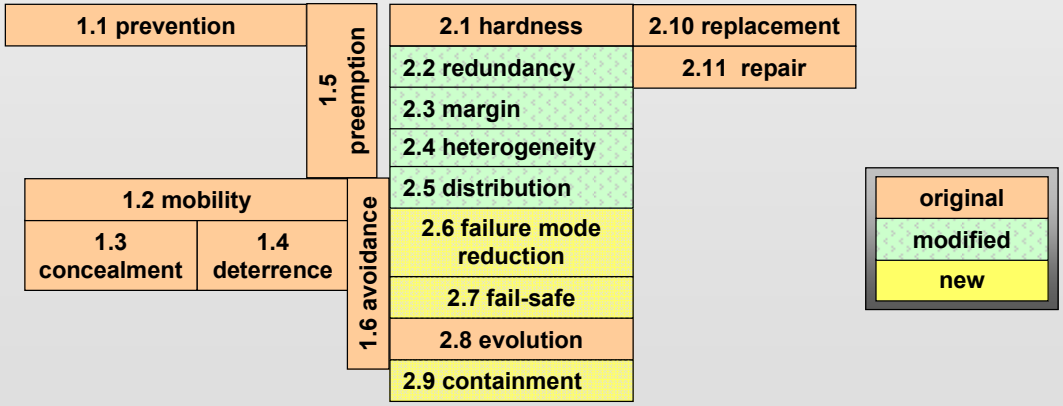


3



4





Source: 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.

Baseline 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	**modify disturbance**
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 disturban	**modify system**
1.5	**preemption**	suppression of an imminent disturbance	
1.6	**avoidance**	maneuverability away from disturbance	
Type II (Reduce Vulnerability)			**Reduce rate or magnitude of degradation**
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	**Enable resilience and recovery**
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	

Lessons from Initial Empirical Tests

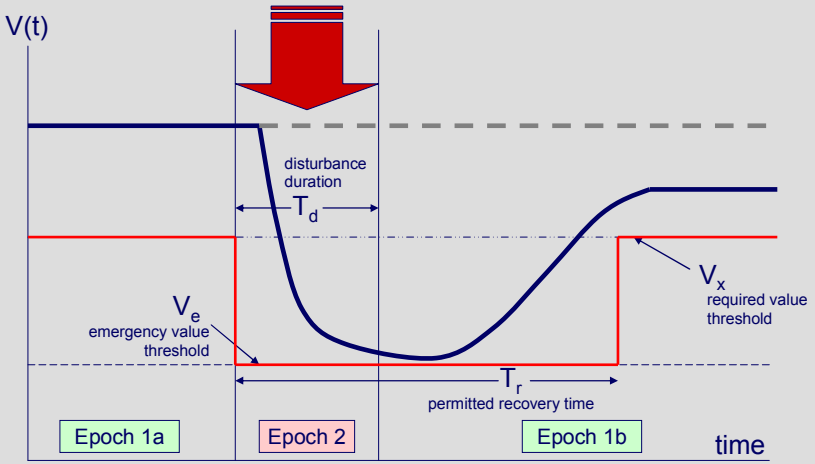
- Valuable iteration between deductive enumeration and inductive empirical testing
- Tension among competing desires
  - Independence
  - Exhaustiveness
  - Maintaining a tractable set
- A-10 and Blackhawk tests expanded number of design principles
  - Three are specializations of original set
    - Heterogeneity
    - Distribution
    - Margin
  - Three inherently new principles
    - Failure mode reduction
    - Fail-safe
    - Containment
  - Net gain of five principles

- Identified **need to conduct more tests** for validation
  - Extensive modifications required after only two empirical tests
  - Future systems should include ***focus on low susceptibility***

Test #1 – F-16C Fighting Falcon

- Multi-role, single-engine, tactical aircraft
- ***Design emphasis on maneuverability***
  - Small size with 9g turn capability, thrust-to-weight ratio >1, exploits vortex lift with cropped delta wings
- Achieved 72-0 combat record
- Introduced in 1974; plans to remain in service by US Air Force until 2025
- Over 4,000 units built and in use by over 24 countries
- Lockheed Martin remains active in F-16 export market

Mapping to Survivability Framework



Unit of Analysis: piloted F-16C vehicle

Disturbances: guns/missiles from air/ground platforms

Required Value Threshold: safe and successful mission

Emergency Value Threshold: crew and vehicle exit from combat zone

F-16C Fighting Falcon

high density

Design Principles

	Sample Survivability Features	Type I (Reduce Susceptibility)						Type II (Reduce Vulnerability)											
		prevention	mobility	concealment	deterrence	preemption	avoidance	hardness	redundancy	margin	heterogeneity	distribution	reduction	fail-safe	evolution	containment	replacement	repair	ODA - exclusive
structure	small visual IR and RF signature (50 x 31 x 16 ft)			X															
	sustains 9-g turns		X				X	X											
	two-tone grey camouflage (standard)			X															
	tail and wing proximity for enhanced maneuverability		X				X												
	blended wing fuselage to reduce transonic drag		X	X			X												
cockpit	situational awareness data link																		X
	autonomous precision targeting (if necessary)	X			X	X							X						
	bubble canopy for enhanced visibility																		X
	cockpit compatibility with night vision goggles			X															
	LANTIRN navigation pod for nighttime operations			X															
	modular avionics																X	X	
	30 degree seat back angle to increase g tolerance							X											
	ACES II ejection seat														X				
propulsion	buried fuel lines			X				X											
	fuel inerting system												X		X	X			
	~29,000-pound engine thrust class		X				X												
	thrust-to-weight ratio >1						X												
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																		
	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															

concealment (passive)

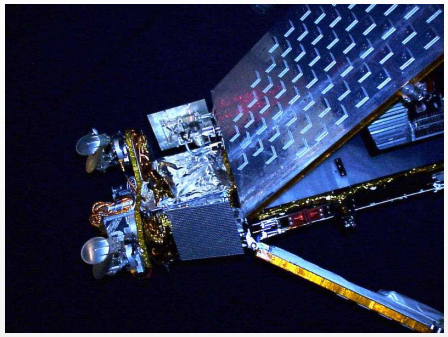
avoidance

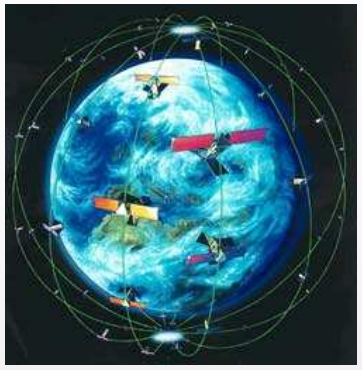
critical system redundancy

concealment (active)

all 17 design principles utilized

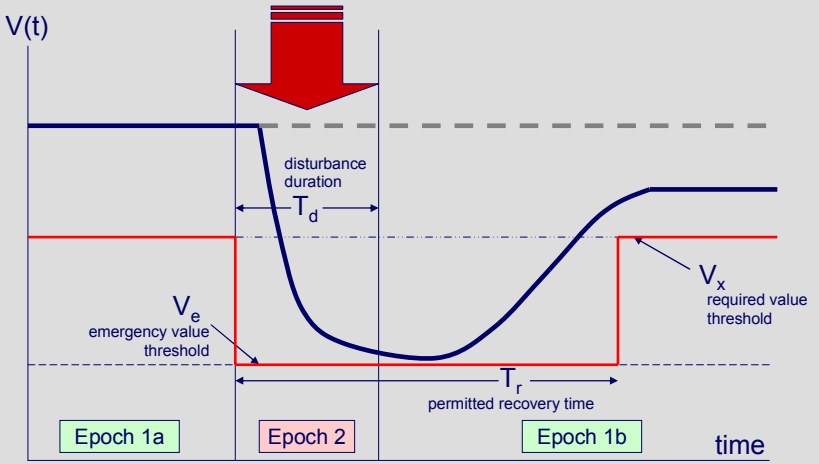
Test #2 – Iridium Telecommunications Network





- Network of 66 interconnected satellites, ground stations, gateways, and links
- Although not value-robust, interesting case in terms of physical survivability
- ***Design emphasis on graceful degradation and rapid reconstitution***
  - Satellite level: autonomous safe mode, redundant electronics, fuel reserves
  - Constellation level: dynamic crosslinks, on-orbit satellite spares
- Traditional hardware redundancy spread over many spacecraft

Mapping to Survivability Framework



Unit of Analysis: all supporting elements of communications service

Disturbances: interactions with natural space environment, node removal

Required Value Threshold: 150 ms delay

Emergency Value Threshold: 400 ms delay

Iridium Network

	Sample Survivability Features	Type I (Reduce Susceptibility)						Type II (Reduce Vulnerability)											ODA - exclusive
		prevention	mobility	concealment	deterrence	preemption	avoidance	hardness	redundancy	margin	heterogeneity	distribution	reduction	fail-safe	evolution	containment	replacement	repair	
satellite	spare Motorola/Freescale PowerPC 603E processor								X										
	small exposed cross-sectional area (7 m²) to debris																		
	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							
	only single gateway required for global coverage									X			X	X					
	Backup Control Facility (BCF) in Rome, Italy											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		

Traditional satellite survivability techniques

R(5y)=0.58

functional with 36 / 66 nodes removed

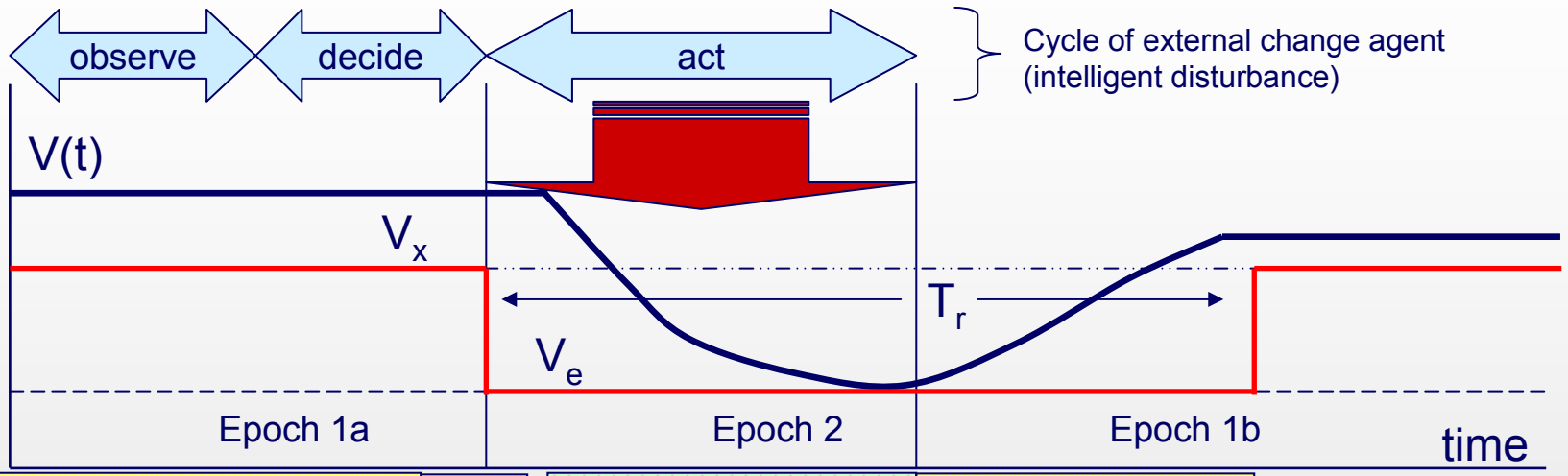
only one ground station required for constellation management

prevention, deterrence, and preemption not utilized in Iridium design


SEA RI
Systems Engineering Advancement Research Initiative

Conclusion

Temporal Mapping of Validated Design Principles



1.1 prevention

1.5 preemption

1.2 mobility

1.3 concealment

1.4 deterrence

1.6 avoidance

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

2.11 repair

Dominant Design Strategy

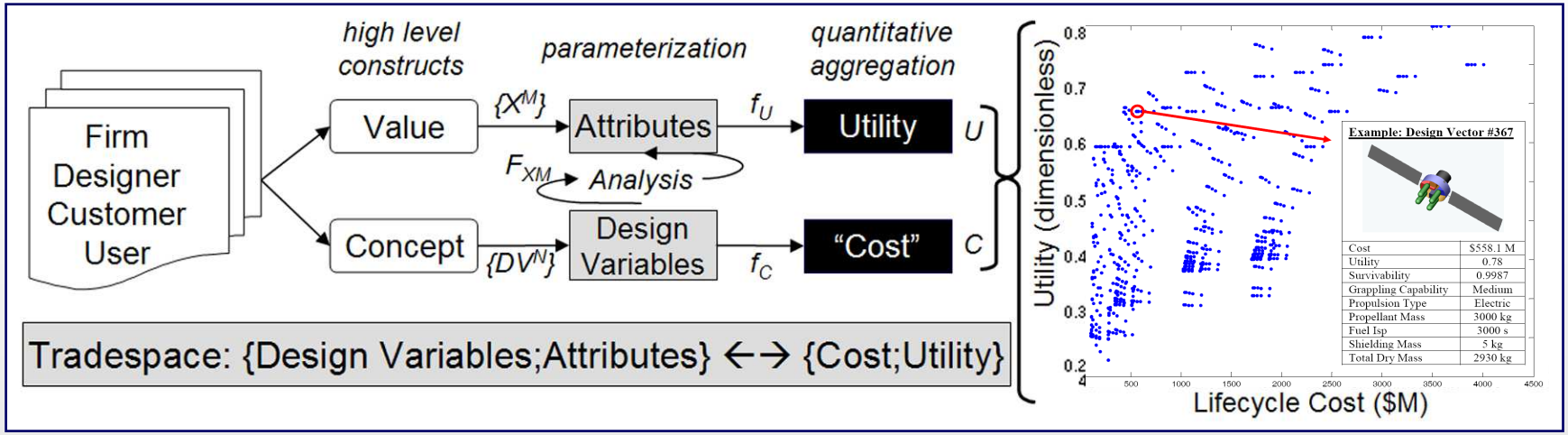
active

passive

Leveraging Design Principles – Dynamic Modeling of Survivability

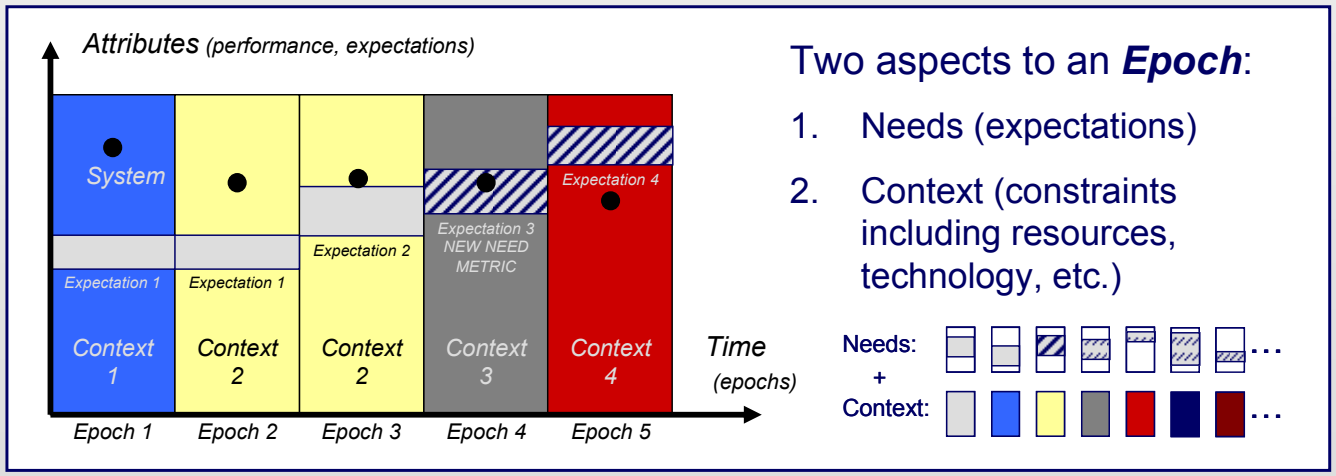
Multi-Attribute Tradespace Exploration (MATE)

(McManus, Hastings and Warmkessel 2004; Ross et al. 2004)



Epoch-Era Analysis

(Ross 2006)



Conclusion

- Design principle framework successfully applied to F-16 and Iridium
  - No survivability features left untraced
  - No taxonomic inconsistencies identified
  - No revisions required of system-disturbance framework

- Four completed empirical test support validity of design principles aerospace domain
  - A-10A Warthog
  - UH-60A Blackhawk
  - F-16C Fighting Falcon
  - Iridium Telecommunications System

  } stratified sample

- Future Work
  - Test validity of design principles in other domains (e.g., transportation)
  - Construct morphological matrix of features across systems
  - Quantification of principles as design variables in dynamic tradespaces

Thank You / Questions?