Two Empirical Tests of Design Principles for Survivable System Architecture

2008 INCOSE Symposium

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

- Introduction
  - Definition of Survivability
  - Motivation for Design Principles
- Empirical Testing
  - Methodology
  - Test #1 – A-10A “Warthog”
  - Test #2 – UH-60A Blackhawk
  - Results
- Synthesis

Introduction

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

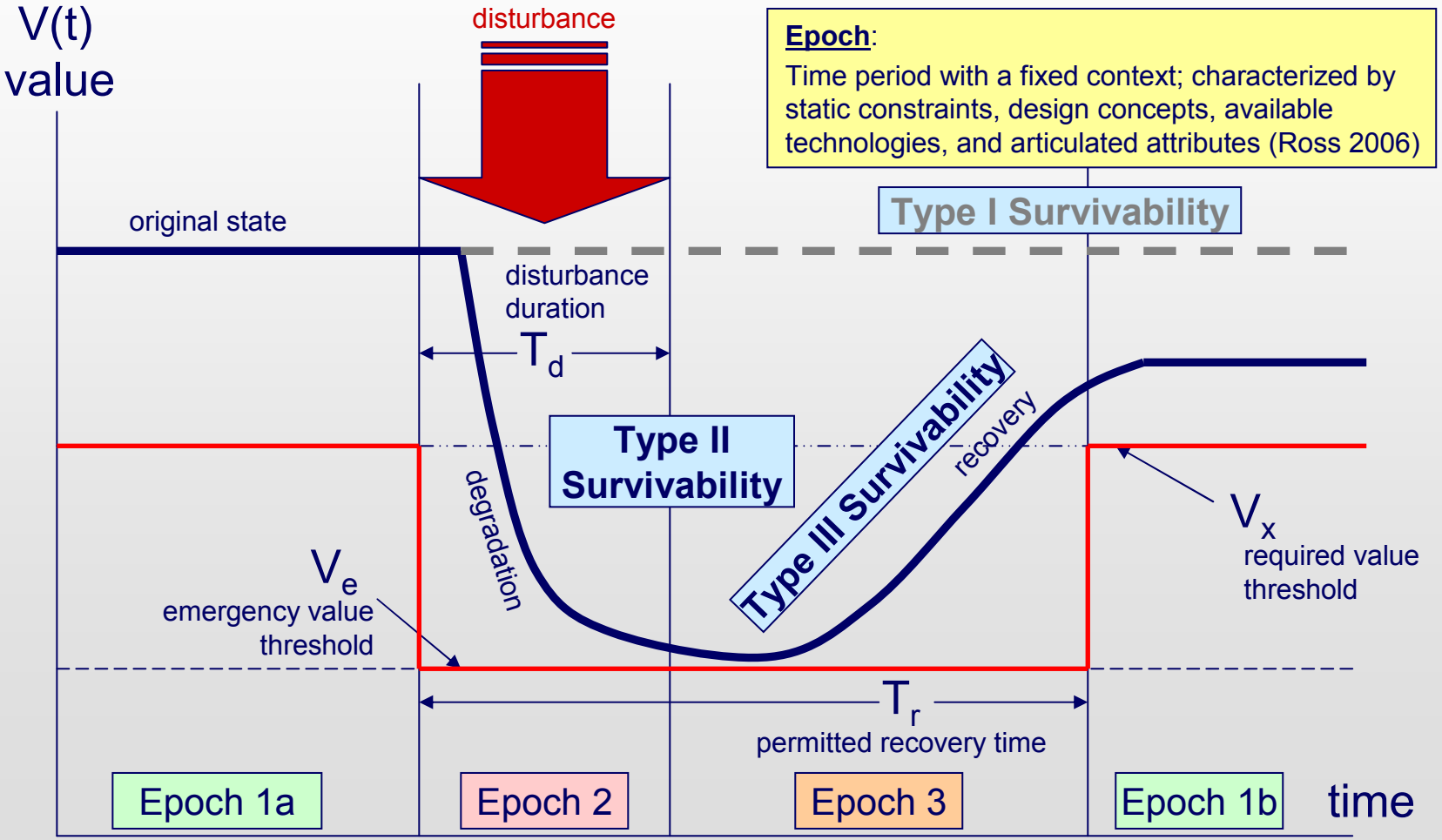
8/28/2005
Hurricane Katrina strikes New Orleans
2000 lives lost
$81.2 billion in damage

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?

Definition of Survivability

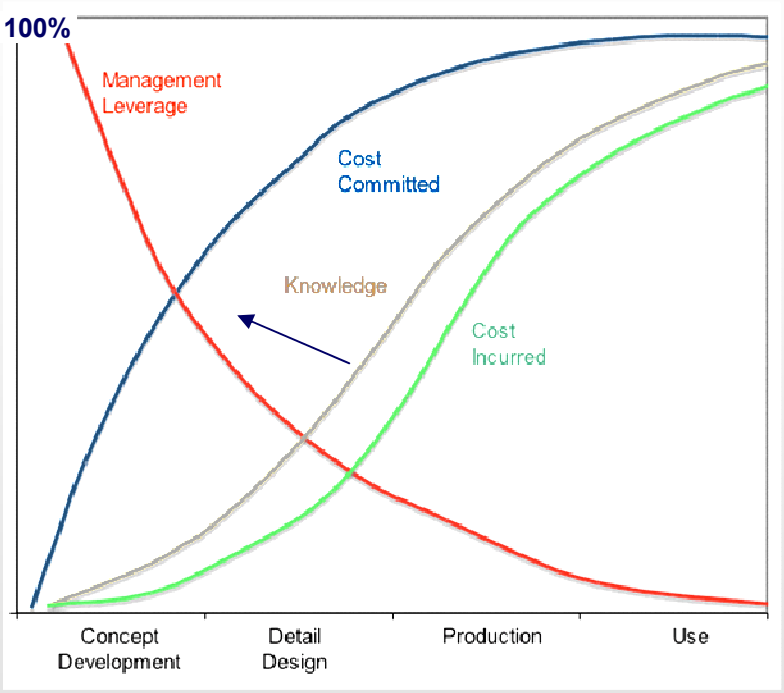
Ability of a system to minimize the impact of a finite-duration disturbance on value delivery through either (I) the reduction of the likelihood or magnitude of a disturbance, (II) the satisfaction of a minimally acceptable level of value delivery during and after a disturbance, and (III) recovery



Motivation for Design Principles: 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)

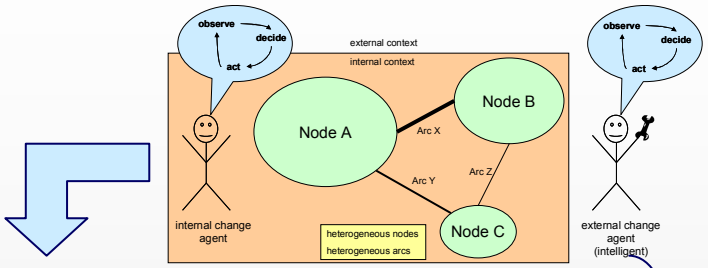
Empirical Testing

Four-Step Methodology (1/4)

Systems Engineering Advancement Research Initiative

Methodology

1. **Deduce design principles from generic system-disturbance representation**



Type I (Reduce Susceptibility)		
1.1	**prevention**	suppression of a future or potential future disturbance
1.2	**mobility**	relocation to avoid detection by an external change agent
1.3	**concealment**	reduction of the visibility of a system from an external change agent
1.4	**deterrence**	dissuasion of a rational external change agent from committing a disturbance
1.5	**preemption**	suppression of an imminent disturbance
1.6	**avoidance**	maneuverability away from disturbance
Type II Survivability (Reduce Vulnerability)		
2.1	**hardness**	resistance of a system to deformation
2.2	**evolution**	alteration of system elements to reduce disturbance effectiveness
2.3	**redundancy**	duplication of critical system components to increase reliability
2.4	**diversity**	variation in system elements (characteristic or spatial) to decrease effectiveness of homogeneous disturbances
Type III Survivability (Increase Resilience)		
3.1	**replacement**	substitution of system elements to improve value delivery
3.2	**repair**	restoration of system to improve value delivery

Literature

Interviews

Cases studies

Four-Step Methodology (2/4)

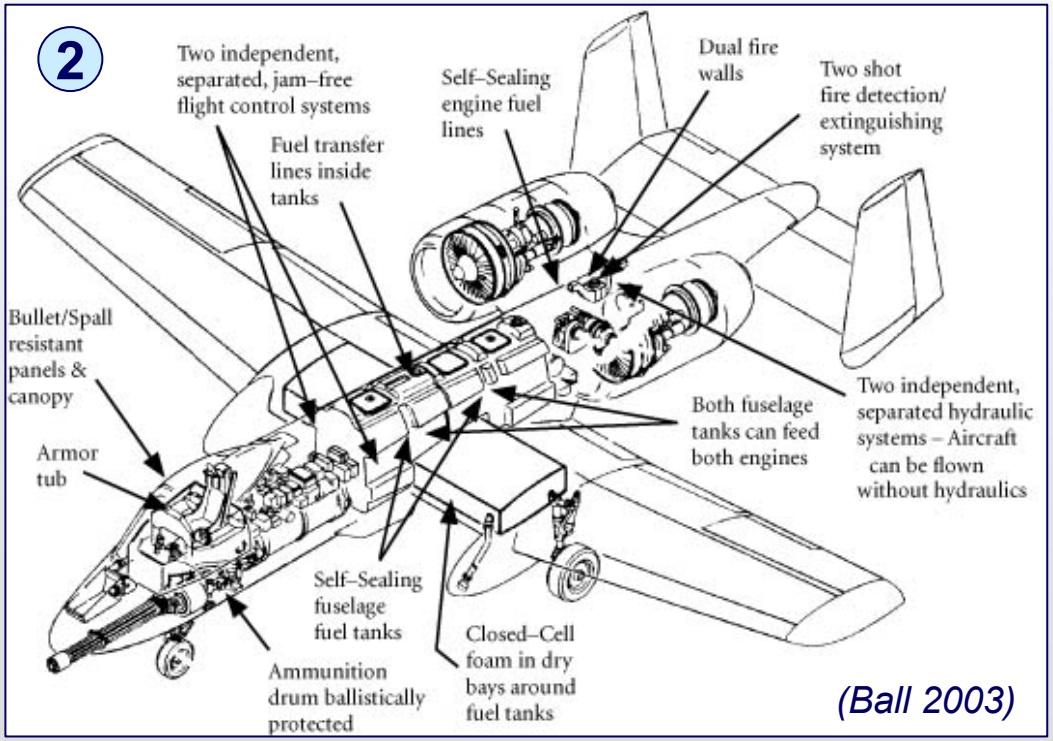
Methodology

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
	Type III Survivability (Increase Resilience)	
3.1	replacement	substitution of system elements to improve value delivery
3.2	repair	restoration of system to improve value delivery

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

Four-Step Methodology (3/4)

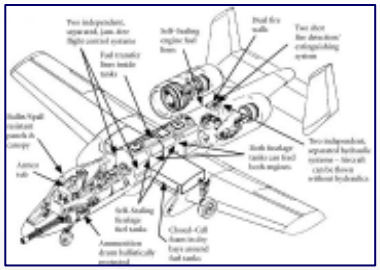
Methodology

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
Type III Survivability (Increase Resilience)		
3.1	**replacement**	substitution of system elements to improve value delivery
3.2	**repair**	restoration of system to improve value delivery

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

Four-Step Methodology (4/4)

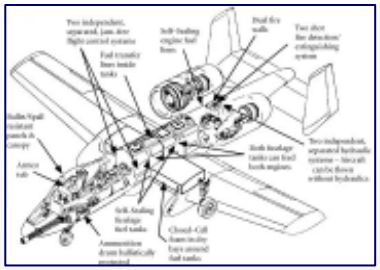
Methodology

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**

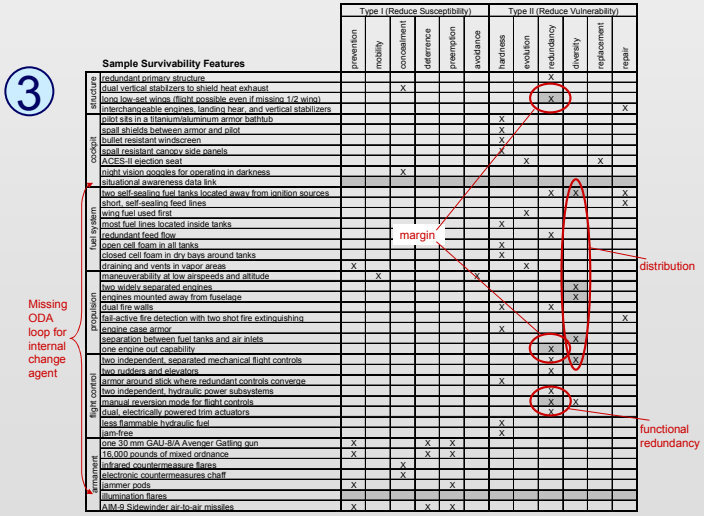
1

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
Type III Survivability (Increase Resilience)		
3.1	**replacement**	substitution of system elements to improve value delivery
3.2	**repair**	restoration of system to improve value delivery

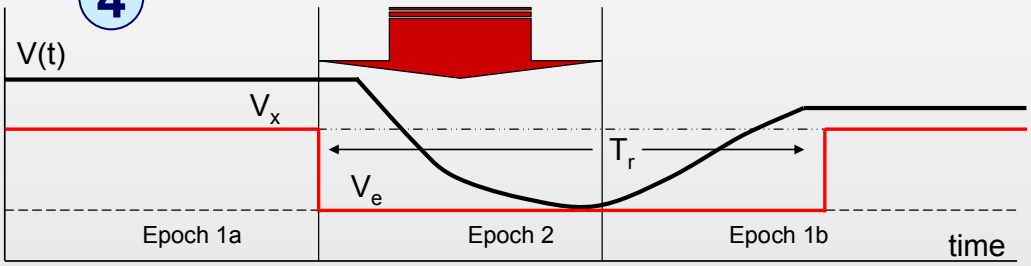
2

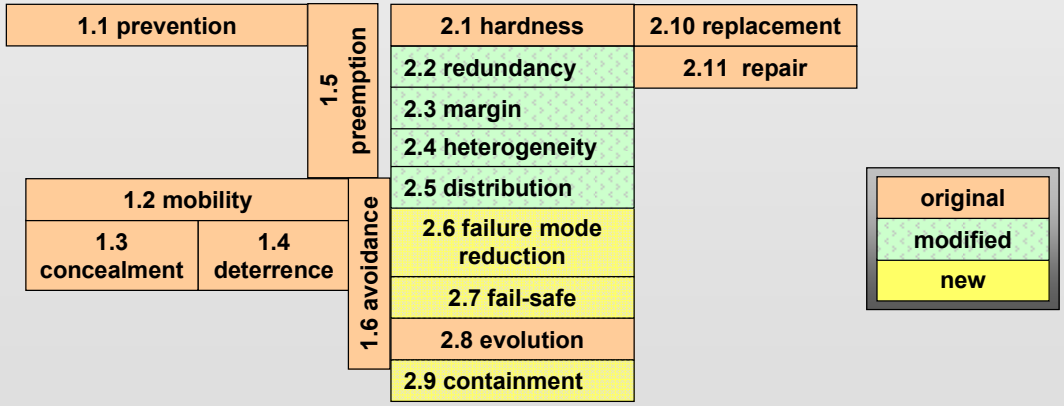


3



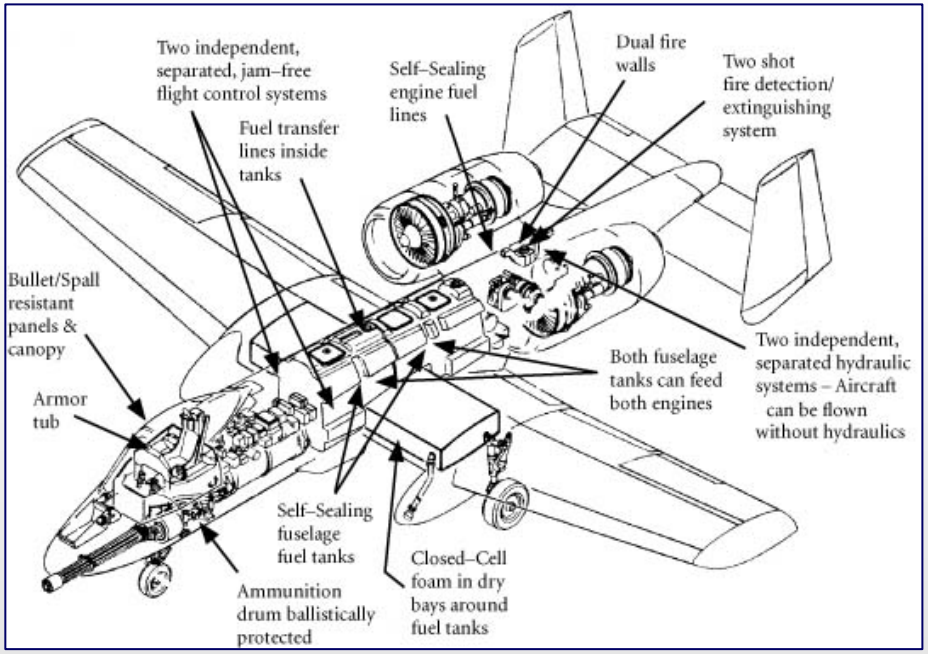
4





Test #1 – A-10A "Warthog"

- Motivation: Vietnam
- First USAF aircraft designed exclusively for close air support
- First USAF aircraft to designed (from inception) to a complete set of survivability requirements
- Validated through extensive combat experience
  - 1st and 2nd Persian Gulf Wars, Kosovo, Afghanistan



Some Vulnerability Reduction Features on the A-10A Thunderbolt II (Ball 2003)

Flying an average of 193 missions per day for 42 days in 1st Gulf War, the A-10 destroyed half of the armor in two Iraqi Republican Guard divisions while losing only six A-10 aircraft and two pilots

A-10A "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					
	closed cell foam in dry bays around tanks							X					
	draining and vents in vapor areas	X							X				
propulsion	maneuverability at low airspeeds and altitude		X				X						
	two widely separated engines										X		
	engines mounted away from fuselage										X		
	dual fire walls							X		X			
	fail-active fire detection with two shot fire extinguishing												X
	engine case armor							X					
	separation between fuel tanks and air inlets										X		
	one engine out capability									X			
flight control	two independent, separated mechanical flight controls									X	X		
	two rudders and elevators									X			
	armor around stick where redundant controls converge							X					
	two independent, hydraulic power subsystems									X			
	manual reversion mode for flight controls									X	X		
	dual, electrically powered trim actuators									X			
	less flammable hydraulic fuel							X					
	jam-free							X					
armament	one 30 mm GAU-8/A Avenger Gatling gun	X			X	X							
	16,000 pounds of mixed ordnance	X			X	X							
	infrared countermeasure flares			X									
	electronic countermeasures chaff			X									
	jammer pods	X				X							
	illumination flares												
	AIM-9 Sidewinder air-to-air missiles	X			X	X							

margin

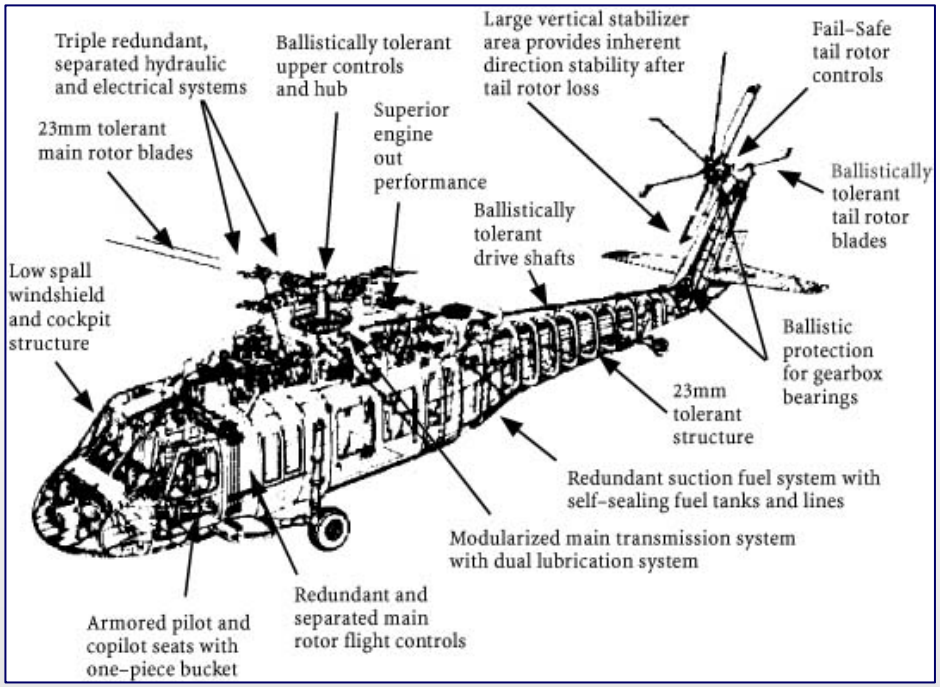
distribution

functional redundancy

Missing ODA loop for internal change agent

Test #2 – UH-60A Blackhawk

- Medium-lift utility or assault helicopter in use by US Army and 20 other military services around the globe
- Firm design requirement on vulnerability reduction
  - Motivated by loss of 2500 helicopters in Vietnam
- Validated through extensive combat experience
  - Served in combat from 1983 Grenada invasion to present day in Iraq



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

Of the 32 Blackhawks used in Grenada, ten were damaged in combat—one helicopter had 45 bullet holes that damaged the rotor blades, fuel tanks, and control systems, yet still managed to complete the mission

UH-60 Blackhawk

Sample Survivability Features

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

containment

fail-safe

margin

failure mode reduction

distribution

Insights from A-10 and UH-60

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

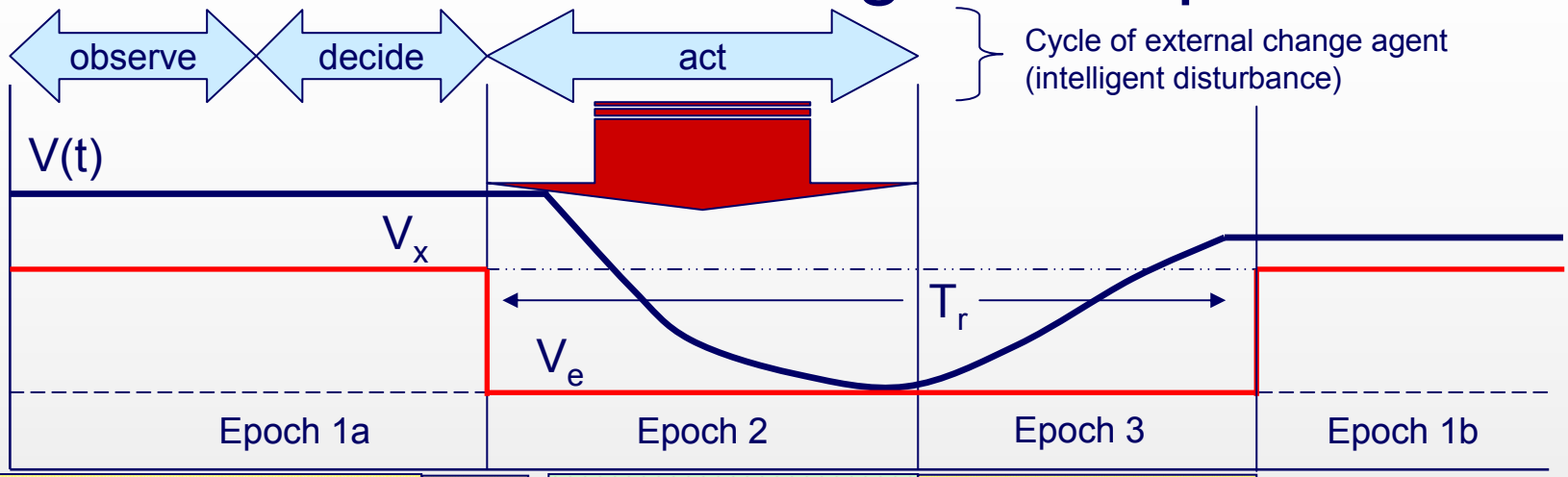
Revised Set of Design Principles

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
Type III Survivability (Increase Resilience)		
2.10	**replacement**	substitution of system elements to improve value delivery
2.11	**repair**	restoration of system to improve value delivery


SEA RI
Systems Engineering Advancement Research Initiative

Synthesis

Temporal Mapping of 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

3.1 replacement
3.2 repair

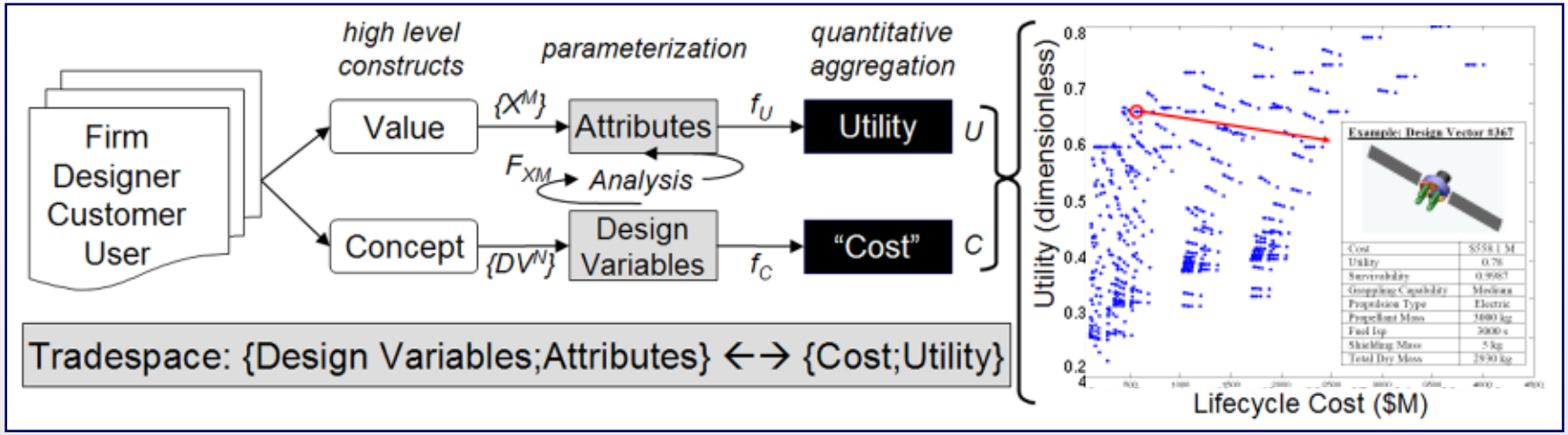
Dominant Design Strategy

active
passive

Leveraging Design Principles – Dynamic Modeling of Survivability

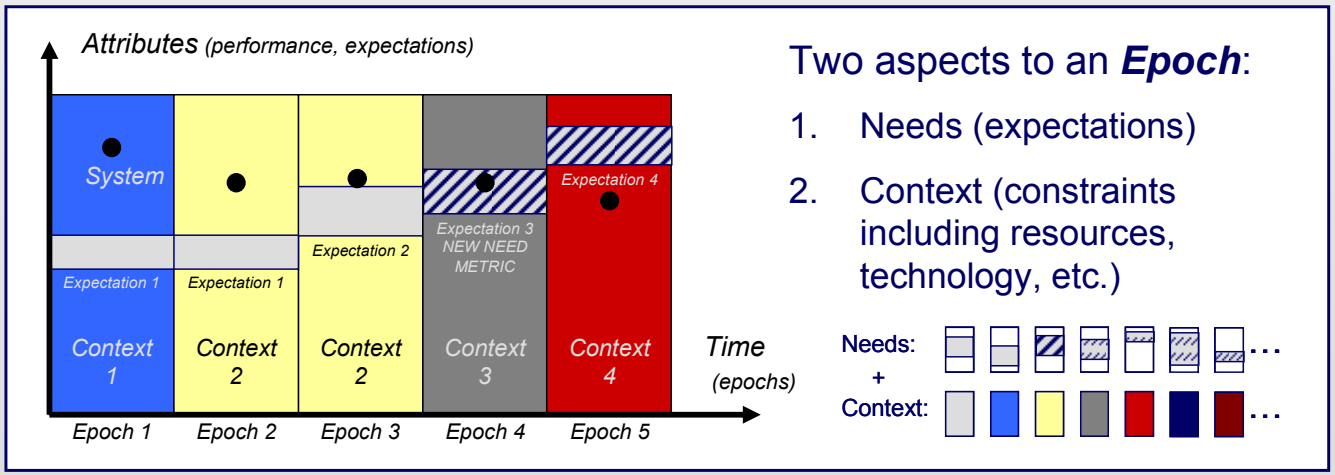
Multi-Attribute Tradespace Exploration (MATE)

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



Epoch-Era Analysis

(Ross 2006)



Two aspects to an ***Epoch***:

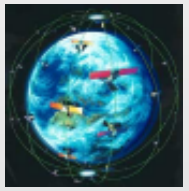
1. Needs (expectations)
2. Context (constraints including resources, technology, etc.)

Conclusions

- Proposed six new 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

Valuable iteration between deductive enumeration and empirical testing

- Identified need to conduct more tests
  - Focus on low susceptibility



- Future work
  - Test validity of design principles in other domains
  - Construct morphological matrix of features across systems
  - Quantification of principles as design variables in dynamic tradespaces

Thank You / Questions?

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

Practical Architectures for Survivable Systems and Networks by Peter G. Neumann (2000)

- U.S. Army Research Laboratory report assesses state of architecting for survivability
  - Scope: distributed systems, systems of systems
  - Identifies several inadequacies with current paradigm

> "Systems and networks with critical survivability requirements are extremely difficult to specify, develop, procure, operate, and maintain."
>
> "The currently existing evaluation criteria frameworks are not yet comprehensively suitable for evaluating highly survivable systems."
>
> "…there is almost no experience in evaluating systems having a collection of independent criteria that might contribute to survivability, and the interactions among different criteria subsets are almost unexplored outside of the context of this report."

- Identifies several challenges requiring future work, including…
  - Generic mission models that can be readily tailored to specific systems to evaluate the adequacy of survivability requirements
  - Families of systems and network topologies that are inherently robust to catastrophic failures

Enumeration of design principles for survivability would be a first step towards development of a generic survivability framework

Related Work

- Survivability enhancement concepts for combat aircraft

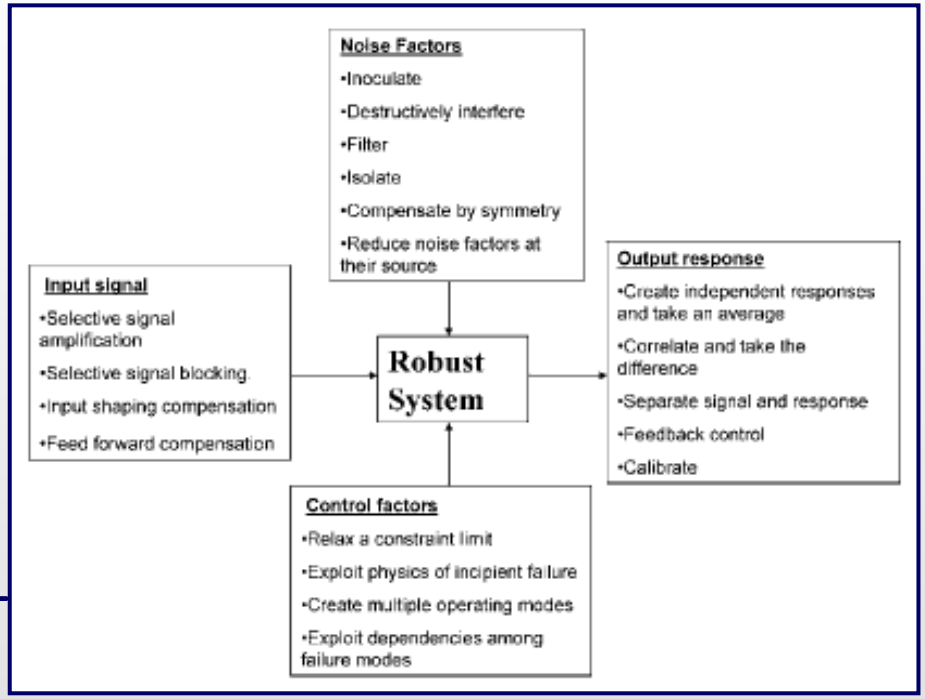
  (Ball 2003)

- 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

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
1.3	**concealment**	reduction of the visibility of a system from an external change agent
1.4	**deterrence**	dissuasion of a rational external change agent from committing a disturbance
1.5	**preemption**	suppression of an imminent disturbance
1.6	**avoidance**	maneuverability away from disturbance
Type II Survivability (Reduce Vulnerability)		
2.1	**hardness**	resistance of a system to deformation
2.2	**evolution**	alteration of system elements to reduce disturbance effectiveness
2.3	**redundancy**	duplication of critical system components to increase reliability
2.4	**diversity**	variation in system elements (characteristic or spatial) to decrease effectiveness of homogeneous disturbances
Type III Survivability (Increase Resilience)		
3.1	**replacement**	substitution of system elements to improve value delivery
3.2	**repair**	restoration of system to improve value delivery

modify system

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

Empirical Testing

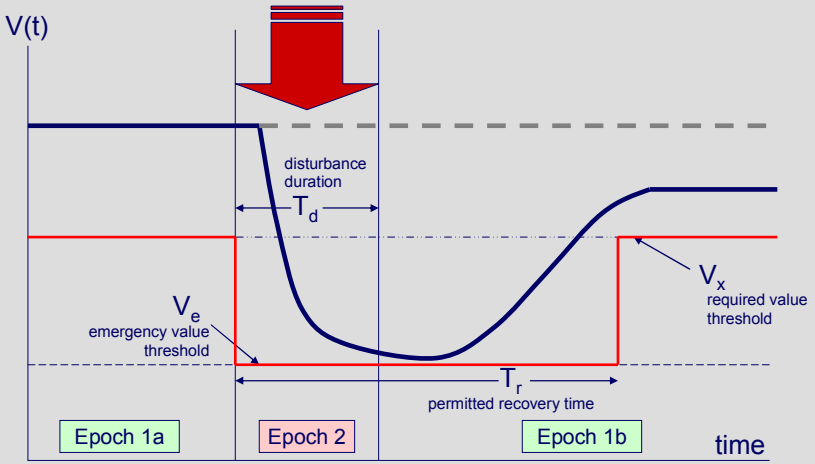
- Motivation
  - Completeness
  - Logical consistency
  - Taxonomic precision
- Methodology
  - Select operational systems with survivability requirements
    - Based on operational performance and access to data
  - Attempt to establish traceability from survivability features in operational systems to 12 general design principles
    - Matrix: survivability features (rows) vs. design principles (columns)
    - Indicate utilization of design principles with “X” marks
  - Evaluate validity
    - Are any survivability features untraced?
    - Does each principle have clear meaning within each domain?
    - Shade problematic areas of matrix in grey to inform improvements

Testing for internal and external validity essential to verifiable, repeatable, and theoretically-sound survivability framework

Test #3 – 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)											ODA - exclusive
		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												
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)

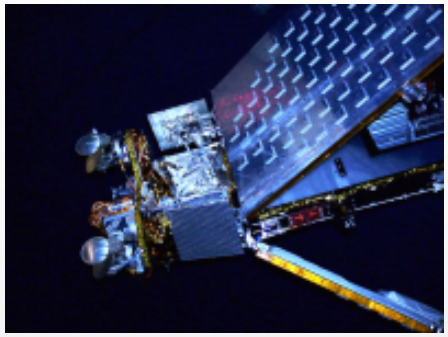
avoidance

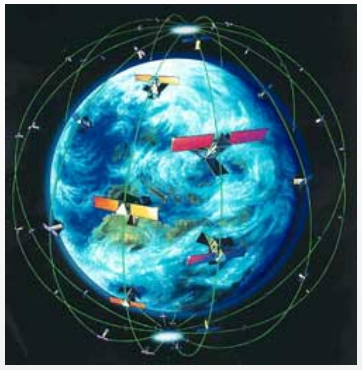
critical system redundancy

concealment (active)

all 17 design principles utilized

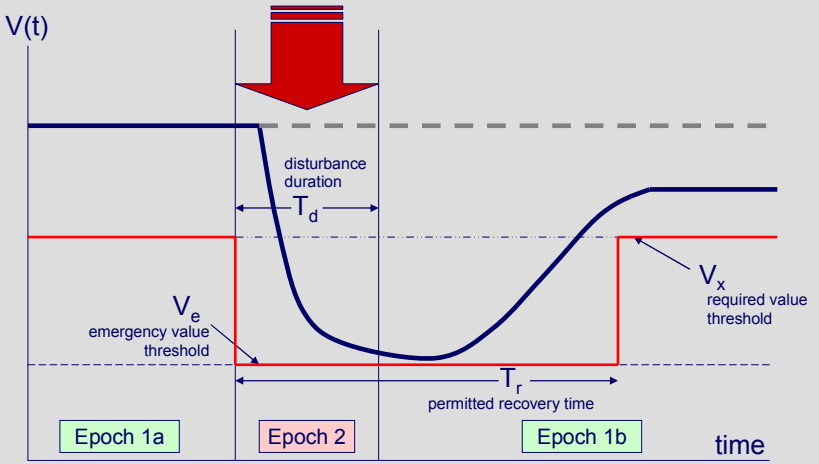
Test #4 – Iridium Telecommunications Network





- 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

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