Systems Engineering Advancement Research Initiative

Survivability Design Principles for Enhanced Concept Generation and Evaluation

19th INCOSE Symposium
Suntec City, Singapore
22 July 2009

Matthew G. Richards, Ph.D.,
Research Assistant, Engineering Systems Division

Adam M. Ross, Ph.D.,
Research Scientist, Engineering Systems Division

Donna H. Rhodes, Ph.D.,
Senior Lecturer, Engineering Systems Division

Daniel E. Hastings, Ph.D.,
Professor, Aeronautics and Astronautics & Engineering Systems

Massachusetts Institute of Technology

Agenda

- Introduction
  - Definition of Survivability
  - Survivability Design Principles
- Methodological Overview
  - Multi-Attribute Tradespace Exploration (MATE) for Survivability
  - Case Application: Satellite Radar
- Synthesis

SEARI

Systems Engineering Advancement Research Initiative

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

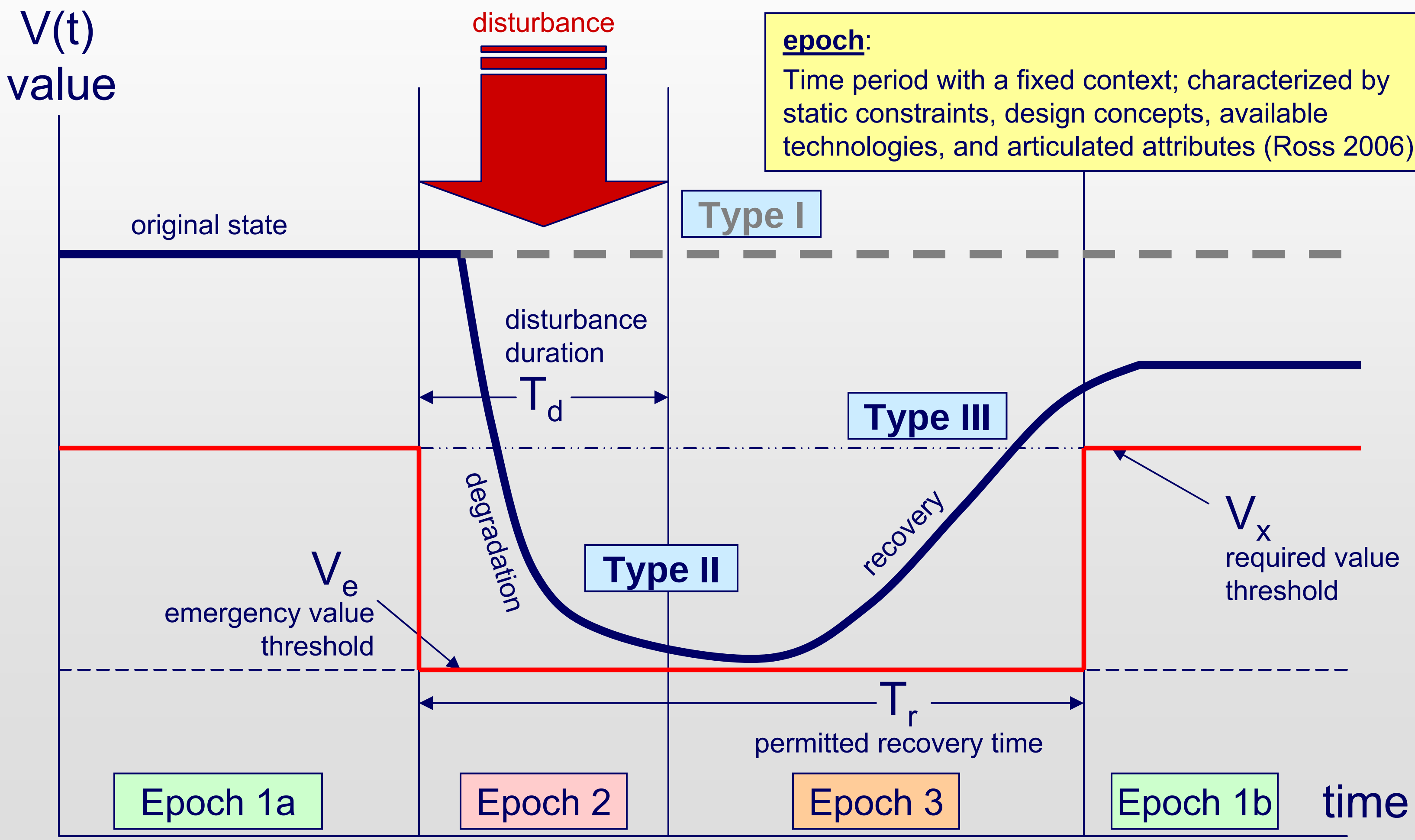
1999 — 2006

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

Definition of Survivability

Ability of a system to minimize the impact of finite-duration disturbances on value delivery through (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/or (III) a timely recovery



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

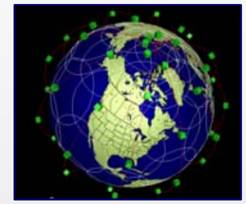
Empirical Generation of Survivability Design Principles

1. Deduce initial design principles from system-disturbance framework, exploratory interviews, and literature (12 design principles)
2. Select operational systems with survivability requirements


A-10A "Warthog"


UH-60A Blackhawk


F-16C Fighting Falcon


Iridium Network

3. Trace design specifications of systems to design principles

Design Principles

	A-10A: Sample Survivability Features	Type I						Type II				Type III	
		prevention	mobility	concealment	deterrence	preemption	avoidance	hardness	evolution	redundancy	diversity	replacement	repair
structure	redundant primary structure									X			
structure	dual vertical stabilizers to shield heat exhaust			X									
structure	long low-set wings (flight possible even if missing 1/2 wing)									X			
structure	interchangeable engines, landing hear, and vertical stabilizers												X

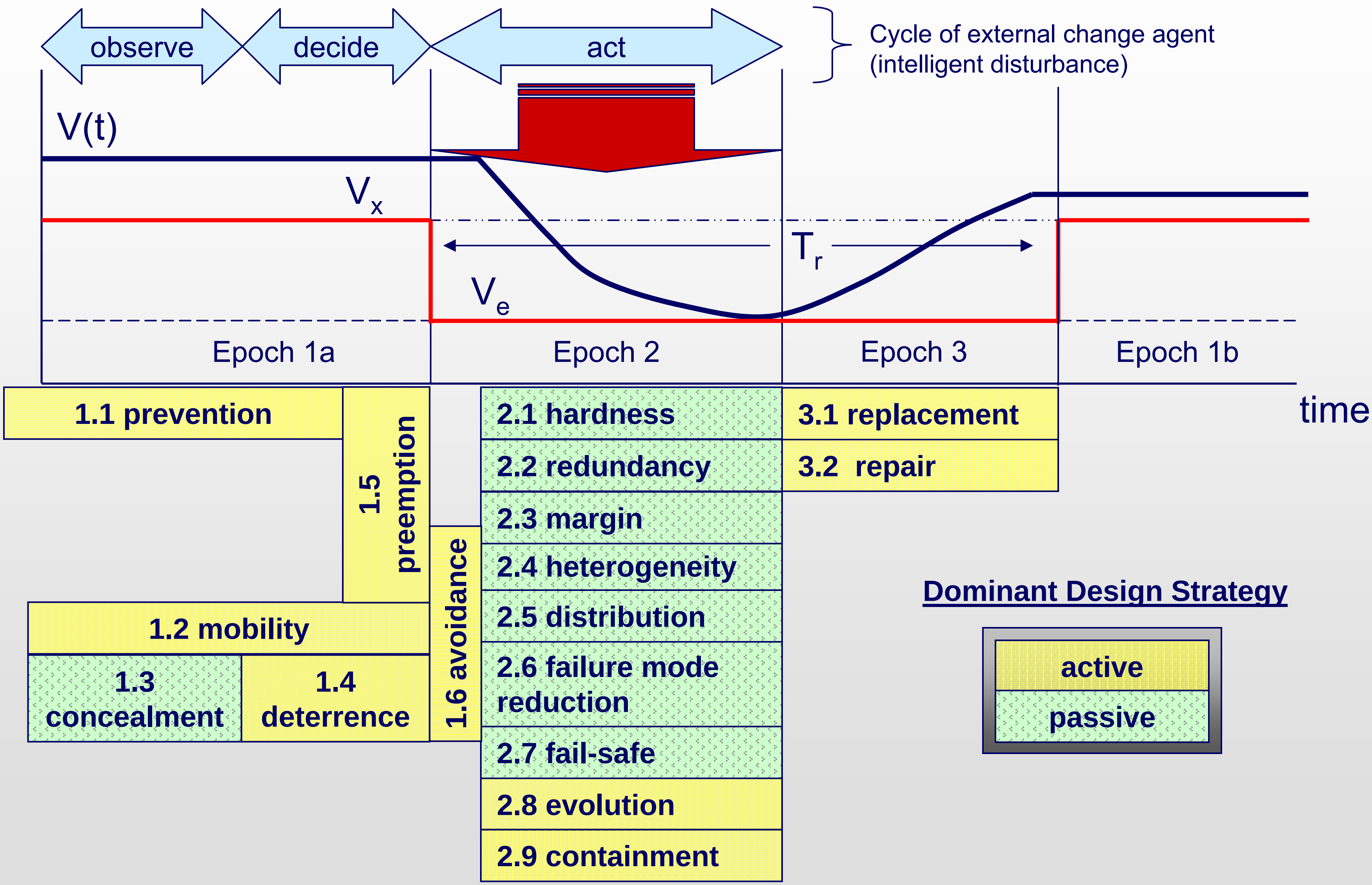
margin

4. Revise set to reflect empirical observation (17 design principles)

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 an ongoing 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 (Enhance Resilience)		
3.1	**replacement**	substitution of system elements to improve value delivery
3.2	**repair**	restoration of system to improve value delivery

Survivability Design Principles

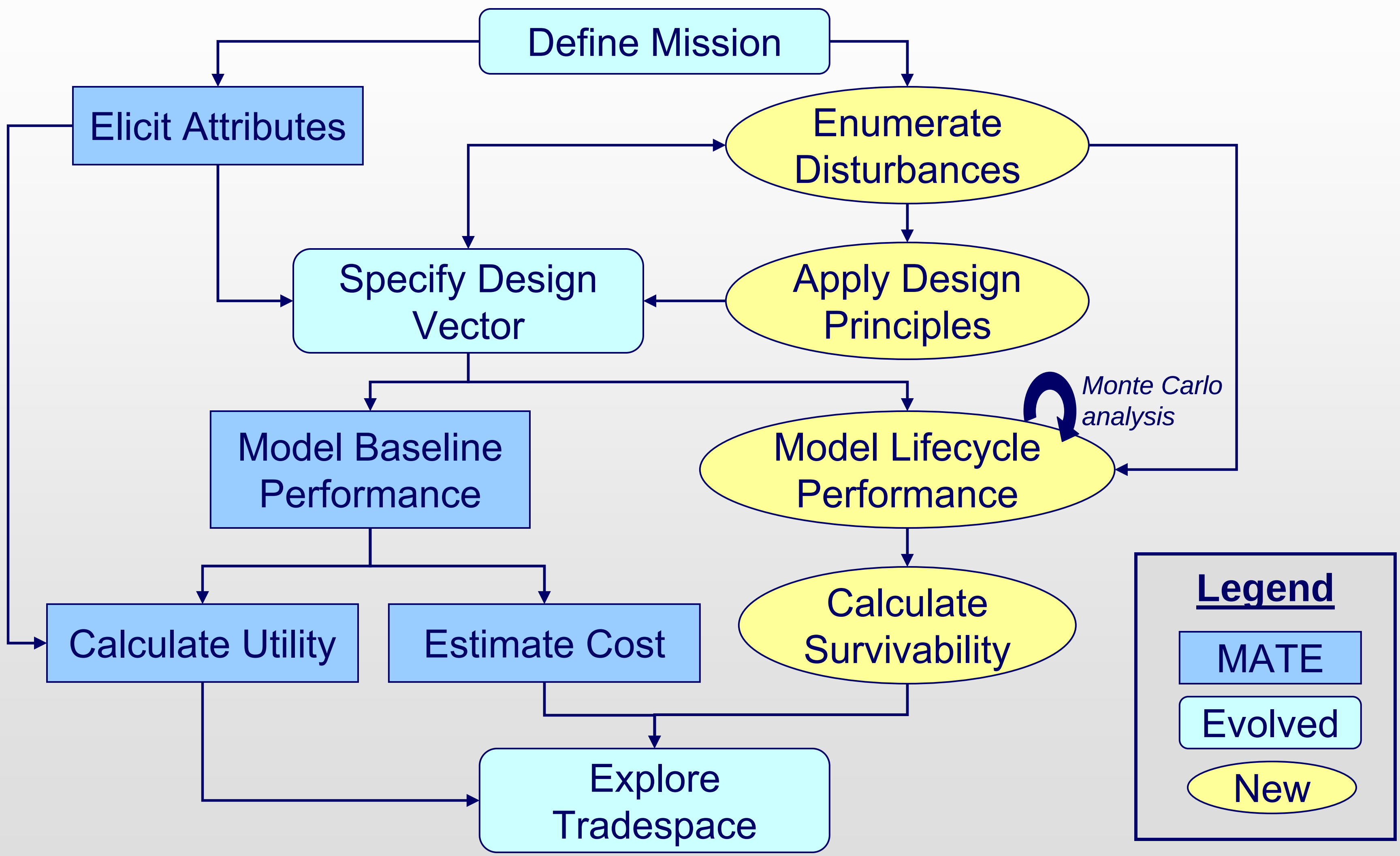


SEA RI

Systems Engineering Advancement Research Initiative

Methodological Overview

Multi-Attribute Tradespace Exploration (MATE) for Survivability



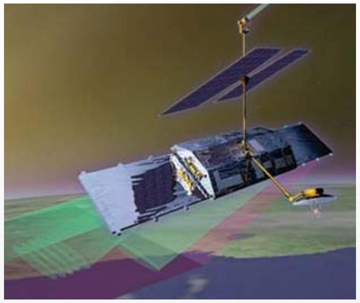
Phases of MATE for Survivability

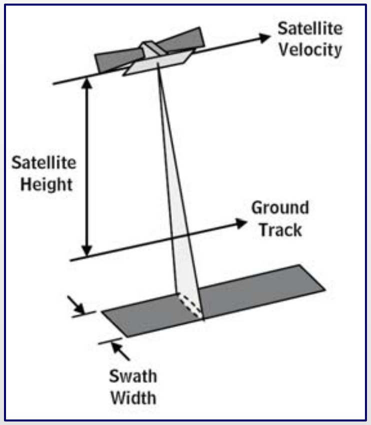
1. **Elicit Value Proposition** – Identify mission statement and quantify decision-maker needs during nominal and emergency states.
2. **Generate Concepts** – Formulate concepts that address decision-maker needs.
3. **Characterize Disturbance Environment** – Develop concept-neutral models of disturbances in operational environment of proposed systems.
4. **Apply Survivability Principles** – Incorporate susceptibility reduction, vulnerability reduction, and resilience enhancement strategies into design vector.
5. **Model Baseline System Performance** – Model and simulate cost and performance of design alternatives to gain an understanding of how decision-maker needs are met in a nominal operational environment.
6. **Model Impact of Disturbances on Lifecycle Performance** – Model and simulate performance of design alternatives across a representative sample of disturbance encounters to gain an understanding of how decision-maker needs are met in perturbed environments.
7. **Apply Survivability Metrics** – Compute time-weighted utility loss and threshold availability for each design alternative as summary statistics for system performance across representative operational lives.
8. **Explore Tradespace** – Perform integrated cost, utility, and survivability trades across design space to identify promising alternatives for more detailed analysis.

Case Application: Satellite Radar

Critical issue in national security space
- Unique all-weather surveillance capability
- Opportunity for impact given ongoing studies
- Rich multi-dimensional tradespace

Unit-of-analysis: SR architecture
- Radar payload
- Constellation of satellites
- Communications network





(CBO 2007)

Case Application Goal

*To assess potential **satellite radar** architectures for providing the United States Military a global, all-weather, on-demand capability to **track moving ground targets**; supporting tactical military operations; maximizing cost-effectiveness; and **surviving disturbances** in the natural space environment.*

Phase 2: Generate Concepts

Design Value Mapping Matrix establishes traceability between value-space and design-space

		ATTRIBUTES															
		Mission											Programmatics				
		Tracking						Imaging					Cost		Schedule		
Variable Name	**Definition Range**	Minimum Target RCS	Min. Detectable Velocity	Number of Target Boxes	Target Acquisition Time	Target Track Life	Tracking Latency	Resolution (Proxy)	Targets per Pass	Field of Regard	Revisit Frequency	Imaging Latency	Baseline Cost	Actual Costs (Era)	Baseline Schedule	Actual Schedule (Era)	**Total Impact**
Peak Transmit Power	1.5 10 20 [KW]	9	9	9	3	1	1	9	9	9	0	1	9	9	9	9	**96**
Radar Bandwidth	.5 1 2 [GHz]	9	9	3	3	1	1	9	9	9	0	1	3	3	3	3	**66**
Radar Frequency	X UHF	9	9	3	3	1	1	9	9	9	0	1	3	3	3	3	**66**
Physical Antenna Area	10 40 100 200 [m^2]	9	9	9	3	1	1	9	9	9	1	1	9	9	9	9	**97**
Receiver Sats per Tx Sat	0 1 2 3 4 5	9	9	3	3	1	1	9	3	3	1	1	9	9	9	9	**79**
Antenna Type	Mechanical vs. AESA	9	9	9	3	3	1	9	9	9	1	1	9	9	9	9	**99**
Satellite Altitude	800 1200 1500 [km]	9	9	3	9	9	3	9	9	9	9	3	1	1	1	1	**85**
Constellation Type	8 Walker IDs	0	0	1	9	9	3	0	0	3	9	3	9	9	9	9	**73**
Comm. Downlink	Relay vs. Downlink	0	0	0	0	0	9	0	0	0	0	9	9	9	3	9	**48**
Tactical Downlink	Yes vs. No	0	0	0	0	3	9	0	0	0	0	9	9	9	3	9	**51**
Processing	Space vs. Ground	0	0	0	1	0	3	1	0	0	0	3	9	9	9	9	**44**
Maneuver Package	1x, 2x, 4x	1	1	1	1	1	0	1	1	1	1	0	9	3	3	3	**27**
Tugable	Yes vs. No	1	1	1	1	1	0	1	1	1	1	0	9	9	9	9	**45**
Constellation Option	none, long-lead, spare	0	0	0	0	0	0	0	0	0	0	0	9	9	9	9	**36**
Total		65	64	42	39	30	33	66	58	62	23	33	106	100	88	100	

DESIGN VARIABLES

Systems Engineering Advancement Research Initiative

Phase 3: Characterize Disturbance Environment

Enumerate disturbances

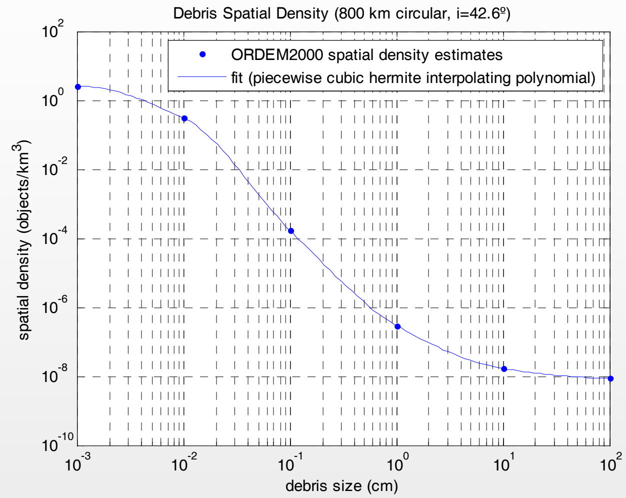
- Orbital debris
- Signal attenuation

Gather data on disturbance magnitude and occurrence

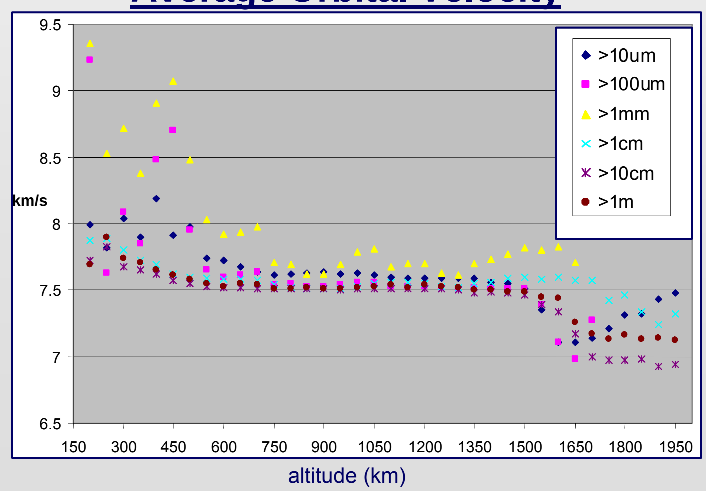
- NASA ORDEM2000 debris model
  - Space Surveillance Network
  - Haystack and Haystack radar data
  - Goldstone radar data
  - Long-Duration Exposure Facility
  - Hubble Telescope array impact data
  - Space Shuttle impact data
  - Mir impact data

Develop system-independent models of disturbance environment

Spatial Density



Average Orbital Velocity



Phase 4: Apply Survivability Principles

Survivability Variable Mapping Matrix establishes traceability between ***environment*** *and* ***design-space***

				disturbances							
	design principles	**concept enhancements**	**design variables (units)**	atmospheric drag fluctuations	arc discharging	high-flux radiation	micrometeorites / debris	signal attenuation	change in target characteristics	failure of relay backbone	loss of tactical ground node
Type I	prevention	reduce exposed s/c area	antenna area (m^2)	9	0	3	9	0	0	0	0
	mobility										
	concealment										
	deterrence										
	preemption										
	avoidance	s/c maneuvering	ΔV (m/s)	9	0	3	1	0	0	0	0
			s/c servicing interface	9	0	1	1	0	0	0	0
		ground receiver maneuverability	mobile receiver	0	0	0	0	3	0	0	3
Type II	hardness	radiation-hardened electronics	hardening (cal/cm^2)	0	3	9	1	0	0	0	0
		bumper shielding	shield thickness (mm)	0	0	0	9	0	0	0	0
	redundancy	duplicate critical s/c functions	bus redundancy	0	1	9	3	0	0	0	0
		on-orbit satellite spares	extra s/c per orbital plan	0	1	3	3	0	3	0	0
		multiple ground receivers	ground infrastructure level	0	0	0	0	3	0	0	9
	margin	over-design power generation	peak transmit power (kW)	0	0	0	3	9	9	0	0
		over-design link budget	assumed signal loss (dB)	0	0	0	0	9	0	0	0
		over-design propulsion system	ΔV (m/s)	3	0	3	0	3	9	0	0
		excess on-board data storage	s/c data capacity (gbits)	0	0	0	0	0	0	3	3
		excess constellation capacity	number of satellites	0	1	3	9	0	0	0	0
	heterogeneity	interface with airborne assets	tactical downlink	3	3	3	3	3	3	3	3
		multiple communication paths	communications downlink	0	0	1	1	9	0	9	3
			tactical downlink	0	0	1	1	9	0	9	3
	distribution	spatial separation of spacecraft	orbital altitude (km)	1	1	3	3	0	9	0	0
		spatial separation of s/c orbits	number of planes	0	0	3	9	0	1	0	1
	failure mode reduction	reduce s/c complexity	bus redundancy	0	0	9	0	0	0	0	0
	fail-safe	autonomous operations	autonomous control	0	0	0	0	3	0	3	3
	evolution	flexible sensing operations	antenna type	0	0	0	0	3	9	0	0
			radar bandwidth (GHz)	0	0	0	0	9	3	0	0
		retraction of s/c appendages	reconfigurable	0	0	9	3	0	0	0	0
	containment	s/c fault monitoring and response	autonomous control	0	1	3	1	0	0	0	0
T III	replacement	rapid reconstitution	constellation spares	0	1	3	9	0	0	0	0
	repair	on-orbit-servicing	s/c servicing interface	9	1	3	3	0	3	0	0

Phase 4: Apply Survivability Principles

Survivability Variable Mapping Matrix* *establishes traceability between* *environment and design-space

	design principles	concept enhancements	design variables (units)	disturbances: atmospheric drag fluctuations	arc discharging	high-flux radiation	micrometeorites / debris	signal attenuation	change in target characteristics	failure of relay backbone	loss of tactical ground node
Type I	prevention	reduce exposed s/c area	antenna area (m^2)	9	0	3	9	0	0	0	0
	mobility										
	concealment										
	deterrence										
	preemption										
	avoidance	s/c maneuvering	ΔV (m/s)	9	0	3	1	0	0	0	0
			s/c servicing interface	9	0	1	1	0	0	0	0
		ground receiver maneuverability	mobile receiver	0	0	0	0	3	0	0	3
Type II	hardness	radiation-hardened electronics	hardening (cal/cm^2)	0	3	9	1	0	0	0	0
		bumper shielding	shield thickness (mm)	0	0	0	9	0	0	0	0
	redundancy	duplicate critical s/c functions	bus redundancy	0	1	9	3	0	0	0	0
		on-orbit satellite spares	extra s/c per orbital plan	0	1	3	3	0	3	0	0
		multiple ground receivers	ground infrastructure level	0	0	0	0	3	0	0	9
	margin	over-design power generation	peak transmit power (kW)	0	0	0	3	9	9	0	0
		over-design link budget	assumed signal loss (dB)	0	0	0	0	9	0	0	0
		over-design propulsion system	ΔV (m/s)	3	0	3	0	3	9	0	0
		excess on-board data storage	s/c data capacity (gbits)	0	0	0	0	0	0	3	3
		excess constellation capacity	number of satellites	0	1	3	9	0	0	0	0
	heterogeneity	interface with airborne assets	tactical downlink	3	3	3	3	3	3	3	3
		multiple communication paths	communications downlink	0	0	1	1	9	0	9	3
			tactical downlink	0	0	1	1	9	0	9	3
	distribution	spatial separation of spacecraft	orbital altitude (km)	1	1	3	3	0	9	0	0
		spatial separation of s/c orbits	number of planes	0	0	3	9	0	1	0	1
	failure mode reduction	reduce s/c complexity	bus redundancy	0	0	9	0	0	0	0	0
	fail-safe	autonomous operations	autonomous control	0	0	0	0	3	0	3	3
	evolution	flexible sensing operations	antenna type	0	0	0	0	3	9	0	0
			radar bandwidth (GHz)	0	0	0	0	9	3	0	0
		retraction of s/c appendages	reconfigurable	0	0	9	3	0	0	0	0
	containment	s/c fault monitoring and response	autonomous control	0	1	3	1	0	0	0	0
T III	replacement	rapid reconstitution	constellation spares	0	1	3	9	0	0	0	0
	repair	on-orbit-servicing	s/c servicing interface	9	1	3	3	0	3	0	0

Phase 4: Apply Survivability Principles

Survivability Variable Mapping Matrix establishes traceability between environment and design-space

disturbances

	design principles	concept enhancements	design variables (units)	atmospheric drag fluctuations	arc discharging	high-flux radiation	micrometeorites / debris	signal attenuation	change in target characteristics	failure of relay backbone	loss of tactical ground node
Type I	prevention	reduce exposed s/c area	antenna area (m^2)	9	0	3	9	0	0	0	0
Type I	mobility										
Type I	concealment										
Type I	deterrence										
Type I	preemption										
Type I	avoidance	s/c maneuvering	ΔV (m/s)	9	0	3	1	0	0	0	0
Type I	avoidance	s/c maneuvering	s/c servicing interface	9	0	1	1	0	0	0	0
Type I	avoidance	ground receiver maneuverability	mobile receiver	0	0	0	0	3	0	0	3
Type II	hardness	radiation-hardened electronics	hardening (cal/cm^2)	0	3	9	1	0	0	0	0
Type II	hardness	bumper shielding	shield thickness (mm)	0	0	0	9	0	0	0	0
Type II	redundancy	duplicate critical s/c functions	bus redundancy	0	1	9	3	0	0	0	0
Type II	redundancy	on-orbit satellite spares	extra s/c per orbital plan	0	1	3	3	0	3	0	0
Type II	redundancy	multiple ground receivers	ground infrastructure level	0	0	0	0	3	0	0	9
Type II	margin	over-design power generation	peak transmit power (kW)	0	0	0	3	9	9	0	0
Type II	margin	over-design link budget	assumed signal loss (dB)	0	0	0	0	9	0	0	0
Type II	margin	over-design propulsion system	ΔV (m/s)	3	0	3	0	3	9	0	0
Type II	margin	excess on-board data storage	s/c data capacity (gbits)	0	0	0	0	0	0	3	3
Type II	margin	excess constellation capacity	number of satellites	0	1	3	9	0	0	0	0
Type II	heterogeneity	interface with airborne assets	tactical downlink	3	3	3	3	3	3	3	3
Type II	heterogeneity	multiple communication paths	communications downlink	0	0	1	1	9	0	9	3
Type II	heterogeneity	multiple communication paths	tactical downlink	0	0	1	1	9	0	9	3
Type II	distribution	spatial separation of spacecraft	orbital altitude (km)	1	1	3	3	0	9	0	0
Type II	distribution	spatial separation of s/c orbits	number of planes	0	0	3	9	0	1	0	1
Type II	failure mode reduction	reduce s/c complexity	bus redundancy	0	0	9	0	0	0	0	0
Type II	fail-safe	autonomous operations	autonomous control	0	0	0	0	3	0	3	3
Type II	evolution	flexible sensing operations	antenna type	0	0	0	0	3	9	0	0
Type II	evolution	flexible sensing operations	radar bandwidth (GHz)	0	0	0	0	9	3	0	0
Type II	evolution	retraction of s/c appendages	reconfigurable	0	0	9	3	0	0	0	0
Type II	containment	s/c fault monitoring and response	autonomous control	0	1	3	1	0	0	0	0
T III	replacement	rapid reconstitution	constellation spares	0	1	3	9	0	0	0	0
T III	repair	on-orbit-servicing	s/c servicing interface	9	1	3	3	0	3	0	0

finalized design vector

(n=3888)

Orbit Altitude (km)
800
1500

Peak Transmit Power (kW)
1.5
10
20

Walker ID
5/5/1
9/3/2
27/3/1
66/6/5

Radar Bandwidth (MHz)
500
1000
2000

Antenna Area (m^2)
10
40
100

Comm. Architecture
Direct Downlink Only
Relay Backbone

Phase 4: Apply Survivability Principles

Survivability Variable Mapping Matrix establishes traceability between environment and design-space

disturbances

Type	design principles	concept enhancements	design variables (units)	atmospheric drag fluctuations	arc discharging	high-flux radiation	micrometeorites / debris	signal attenuation	change in target characteristics	failure of relay backbone	loss of tactical ground node
Type I	prevention	reduce exposed s/c area	antenna area (m^2)	9	0	3	9	0	0	0	0
Type I	mobility										
Type I	concealment										
Type I	deterrence										
Type I	preemption										
Type I	avoidance	s/c maneuvering	ΔV (m/s)	9	0	3	1	0	0	0	0
Type I			s/c servicing interface	9	0	1	1	0	0	0	0
Type I		ground receiver maneuverability	mobile receiver	0	0	0	0	3	0	0	3
Type II	hardness	radiation-hardened electronics	hardening (cal/cm^2)	0	3	9	1	0	0	0	0
Type II		bumper shielding	shield thickness (mm)	0	0	0	9	0	0	0	0
Type II	redundancy	duplicate critical s/c functions	bus redundancy	0	1	9	3	0	0	0	0
Type II		on-orbit satellite spares	extra s/c per orbital plan	0	1	3	3	0	3	0	0
Type II		multiple ground receivers	ground infrastructure level	0	0	0	0	3	0	0	9
Type II	margin	over-design power generation	peak transmit power (kW)	0	0	0	3	9	9	0	0
Type II		over-design link budget	assumed signal loss (dB)	0	0	0	0	9	0	0	0
Type II		over-design propulsion system	ΔV (m/s)	3	0	3	0	3	9	0	0
Type II		excess on-board data storage	s/c data capacity (gbits)	0	0	0	0	0	0	3	3
Type II		excess constellation capacity	number of satellites	0	1	3	9	0	0	0	0
Type II	heterogeneity	interface with airborne assets	tactical downlink	3	3	3	3	3	3	3	3
Type II		multiple communication paths	communications downlink	0	0	1	1	9	0	9	3
Type II			tactical downlink	0	0	1	1	9	0	9	3
Type II	distribution	spatial separation of spacecraft	orbital altitude (km)	1	1	3	3	0	9	0	0
Type II		spatial separation of s/c orbits	number of planes	0	0	3	9	0	1	0	1
Type II	failure mode reduction	reduce s/c complexity	bus redundancy	0	0	9	0	0	0	0	0
Type II	fail-safe	autonomous operations	autonomous control	0	0	0	0	3	0	3	3
Type II	evolution	flexible sensing operations	antenna type	0	0	0	0	3	9	0	0
Type II			radar bandwidth (GHz)	0	0	0	0	9	3	0	0
Type II		retraction of s/c appendages	reconfigurable	0	0	9	3	0	0	0	0
Type II	containment	s/c fault monitoring and response	autonomous control	0	1	3	1	0	0	0	0
T III	replacement	rapid reconstitution	constellation spares	0	1	3	9	0	0	0	0
T III	repair	on-orbit-servicing	s/c servicing interface	9	1	3	3	0	3	0	0

finalized design vector

(n=3888)

Orbit Altitude (km)
800
1500

Peak Transmit Power (kW)
1.5
10
20

Walker ID
5/5/1
9/3/2
27/3/1
66/6/5

Radar Bandwidth (MHz)
500
1000
2000

Antenna Area (m^2)
10
40
100

Comm. Architecture
Direct Downlink Only
Relay Backbone

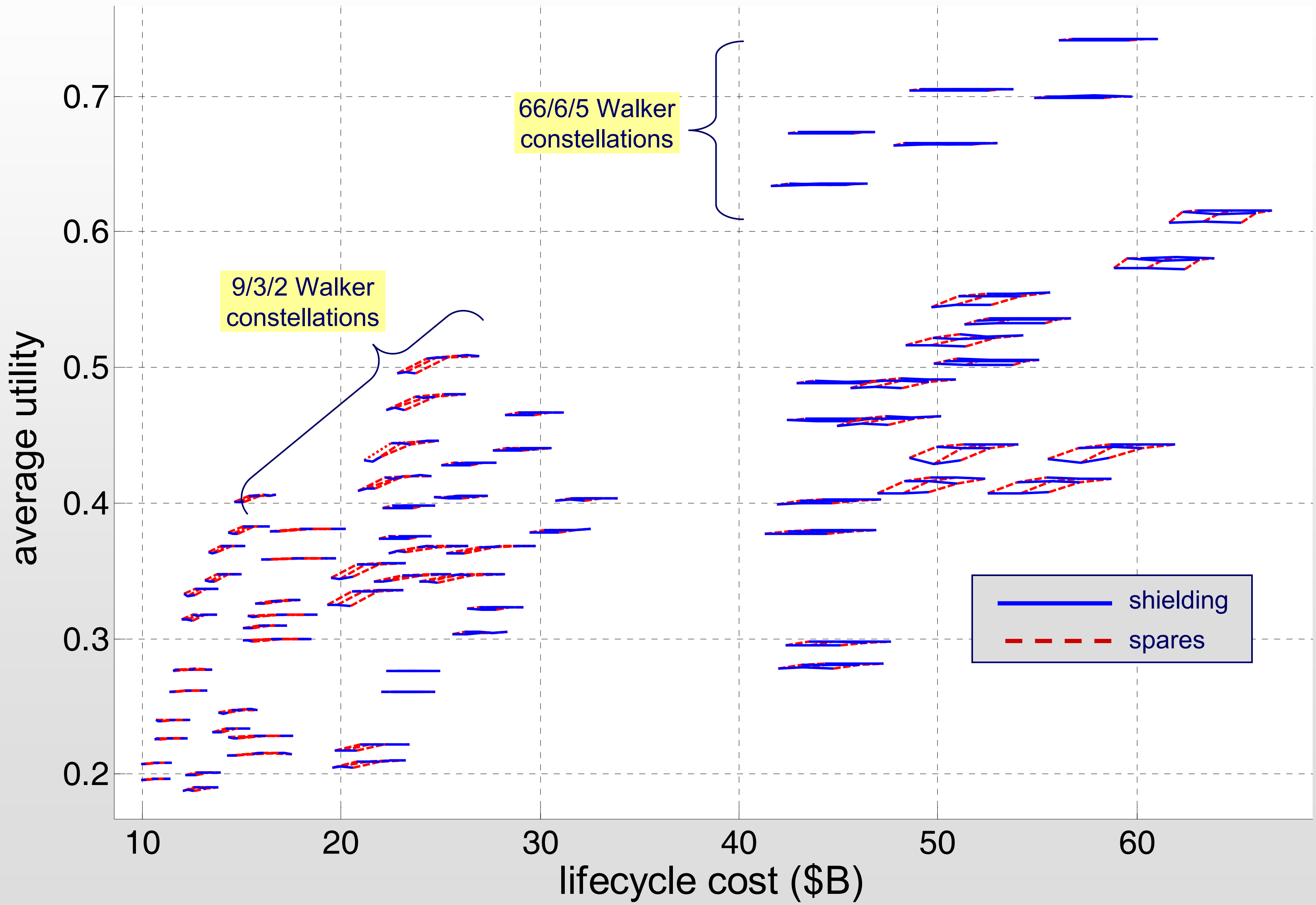
survivability variables

Constellation Spares
0
1
2

Shield Thickness (mm)
1
5
10

Sample Tradespace Output

Response Surfaces for Survivability Design Variables



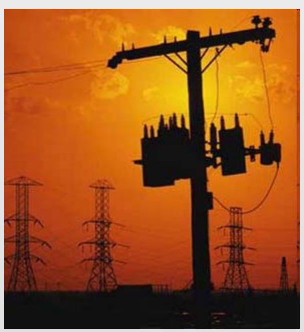
Synthesis

Conclusions

- Survivability definition provides a ***solution-generating*** and ***decision-making*** framework, enabling discovery of systems robust to finite-duration disturbances
- Design principles reveal latent survivability trades in baseline design vector
- Design principles inform selection of additive survivability design variables
- Uniting ***tradespace exploration*** with ***survivability analysis*** generates knowledge that may ultimately lead to better design decisions
- Importance of survivability will grow as critical infrastructures become increasingly large-scale, long-lived, and interdependent

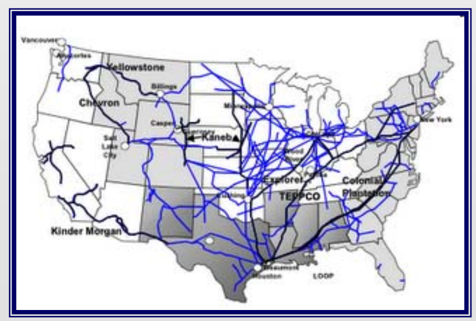
Future Work

- Methodological improvements
  - Parameterize concept-of-operations in design vector
  - Extend scope for systems-of-systems (SoS) engineering
- Apply MATE for Survivability to additional systems for prescriptive insights

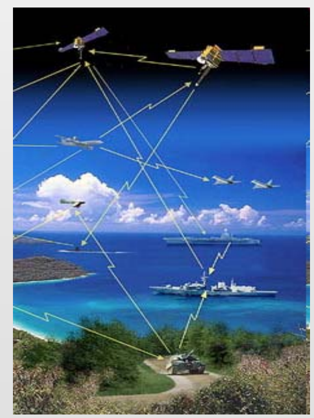


power distribution

transportation



water distribution



communications

SEA RI

Systems Engineering Advancement Research Initiative

Questions?