# Defining Survivability for Engineering Systems

## 2007 Conference on Systems Engineering Research


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

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

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

Annalisa Weigel, Ph.D.
*Professor, Aeronautics and Astronautics & Engineering Systems*
*Massachusetts Institute of Technology*


© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology

# Agenda

- Motivation
  - Observations
  - National Studies
  - Resilience Engineering
- Scope
  - Problem Statement
  - Research Questions
  - Survivability Definition
- Next Steps
  - Relevant Disciplines
  - Research Design

© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology

# Motivation – Observations

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

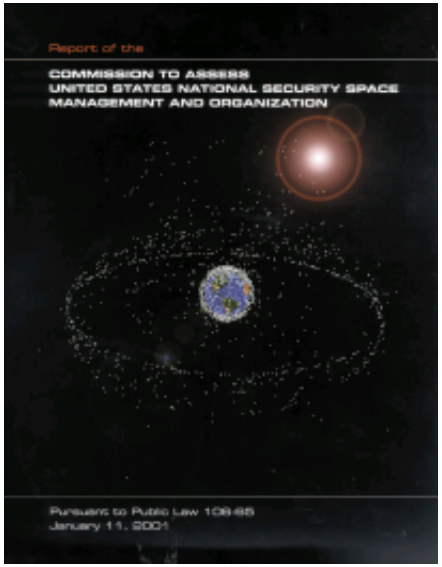
1999 — 2006

9/11/2001
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

© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology

# Motivation – National Studies



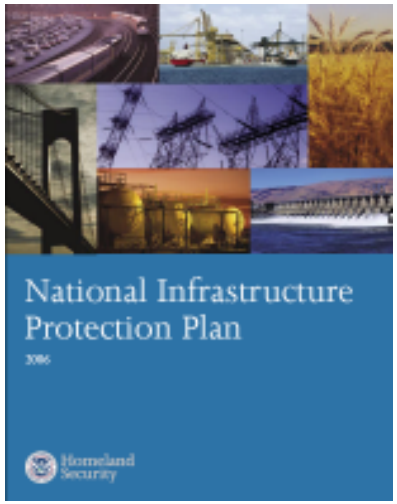

## 2001 Rumsfeld Space Commission

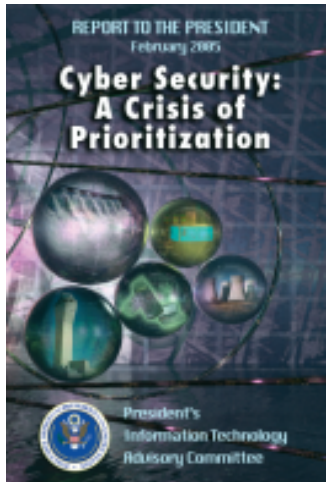
- Identified vulnerabilities of USG space assets due to:
  - Denial & Deception
  - Interference
  - Jamming
  - Microsatellites attacks
  - Nuclear detonation
- Discussed surprise attack as "Pearl Harbor in Space"
  - Vulnerability exacerbated by reliance on commercial systems
  - Inadequate Space Situational Awareness for successful crisis resolution

## 100+ Reports on Critical Infrastructure

*(Post 9/11)*

- Severe vulnerabilities in privately-held, yet critical economic infrastructures
  - Banking and finance
  - Transportation
  - Power systems
  - Information and communications
  - Water and food supply




© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology

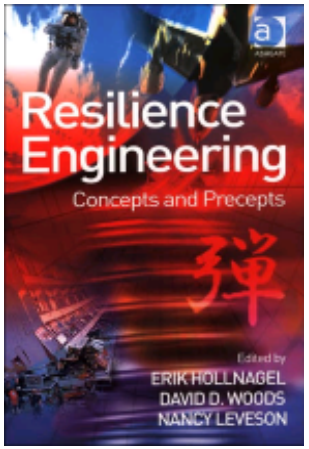
# Motivation – Resilience Engineering

**Brittleness** ← reliability engineering, safety management + Santa Fe, HOT → **Resilience**

## Research Agenda for Systems of Systems (SoS) Architecting

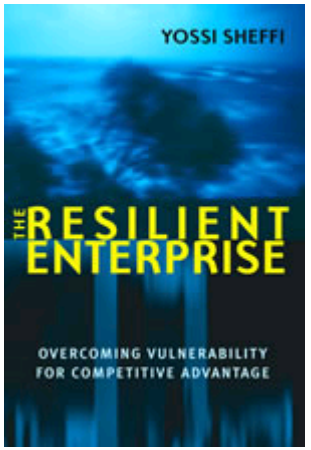
1. Resilience
2. Illustration of Success
3. System vs. SoS Attributes
4. Model Driven Architecting
5. Multiple SoS Architectural Views
6. Human Limits to Handling Complexity
7. Net-Centric Vulnerability
8. Evolution
9. Guided Emergence
10. No Single Owner SoS

***USC Center for Systems and Software Engineering, October 2006***




- Safety emerges from an aggregate of system components, subsystems, software, organizations, human behaviors, and their interactions
- Insufficient for systems to be reliable → need to recover from irregularities
- Posits that traditional safety engineering should extend beyond reactive defenses to design of proactive organization and process

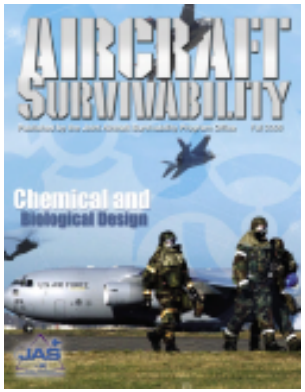
- Drive for efficiency has led to global, lean supply chains that are extremely fragile to disasters
- Empirical data indicates need for balance between security, redundancy, and short-term profits
- Resilient design principles include standardization, modular design, and collaborative relationships with suppliers




© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology

# Research Opportunity

- ***While survivable system design is well understood and best left to established domains…***
  - SMAD → hardening of satellites to natural space radiation, nuclear detonations, directed energy attacks, and jamming
  - Journal of Aircraft Survivability → electronic countermeasures, passive/active protection, situational awareness, suppression of enemy air defenses




- ***Architecting for survivability is a poorly understood, socio-technical issue increasingly relevant to engineering systems***
  - Difficulty in modeling low-probability, high-consequence events
    - Modeling of disturbance frequency and impact
    - Evaluating benefits of protective measures
  - Models of existing survivable architectures are not readily deployable
    - Cold War-era Nuclear Command and Control a national imperative → virtually unlimited resources made available
  - Need for cost/benefit analysis of survivability at architecture level
    - Iridium vs. Milstar → which is more robust?

© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology

# Problem Statement

- Survivability is a non-functional yet critical lifecycle property of engineering systems which must be robust to disturbances

> *As the interdependence of large-scale, distributed systems has grown since the advent of modern telecommunications, so too has the risk from disturbances that rapidly propagate networks, damage critical infrastructure, and trigger catastrophic failures of system-of-systems.*

- Given their network structure, system-of-systems are particularly robust to certain disturbances and particularly fragile to others
- Risks exacerbated by emergence of new sources of disturbances
  - Physical: terrorism
  - Electronic: cyber-attacks
- Research needed to understand the role of survivability as an attribute in engineering system design

© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology

# Research Questions

1. How can survivability be quantified and used as a decision metric in exploring tradespaces during conceptual design of engineering systems?
   a) What is the relationship between survivability and the “ilities” for aerospace systems and how does survivability relate to value robustness?”
   b) Which design principles enable survivability?
   c) How should survivability be traded with cost, performance, schedule, and risk?

2. What are the architectural aspects of designing survivable engineering systems?
   a) How can acquisition of systems with critical survivability requirements be improved?
   b) What supporting infrastructures and cultural attributes—including the network of developers, customers, suppliers, operators, and maintainers—improve lifecycle survivability?

© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology

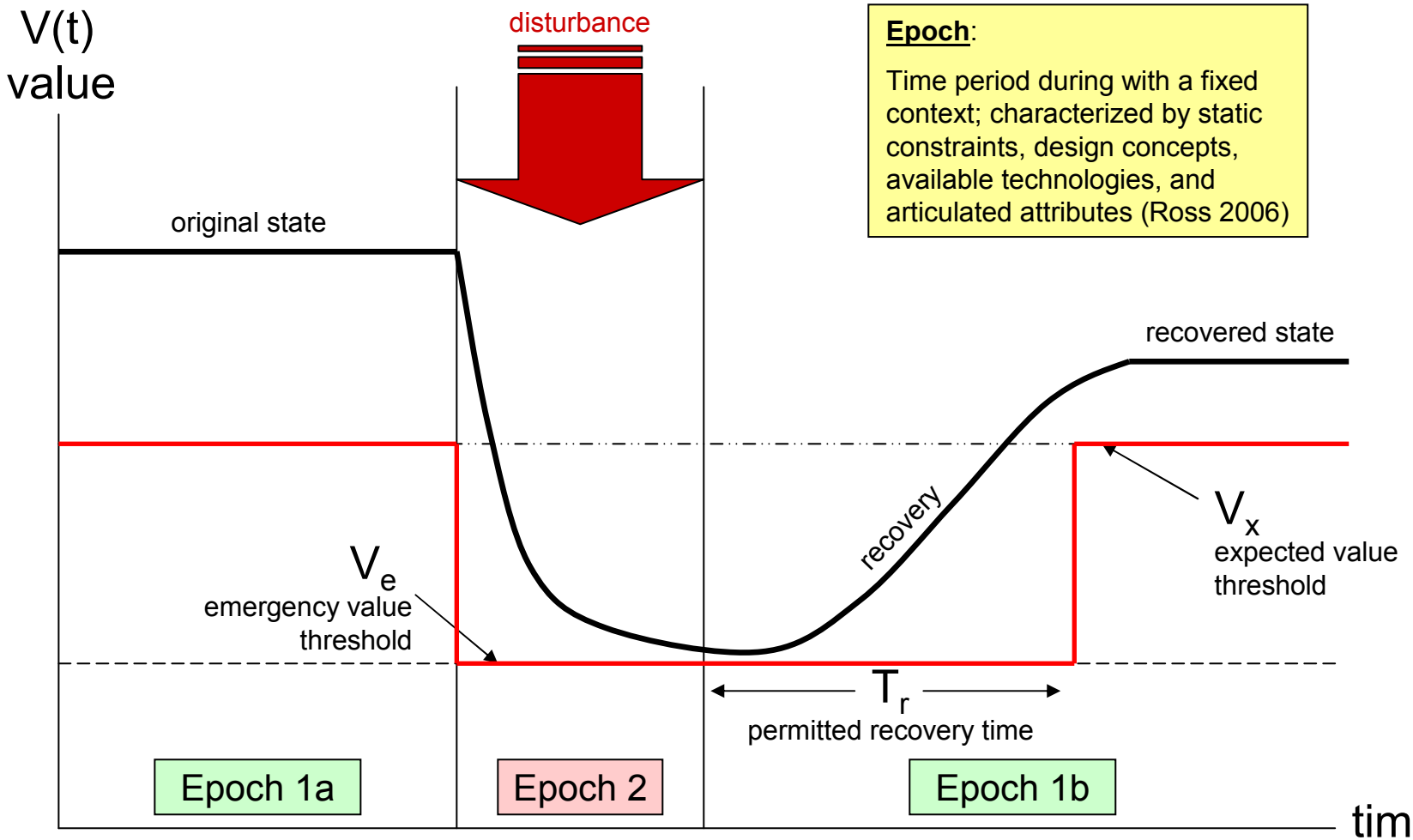
# Definitions of Survivability

| 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 |

© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology

# Definition of Survivability

Ability of a system to minimize the impact of a finite disturbance on value delivery, achieved through either (1) the satisfaction of a minimally acceptable level of value delivery during and after a finite disturbance or (2) the reduction of the likelihood or magnitude of a disturbance




**Epoch**:

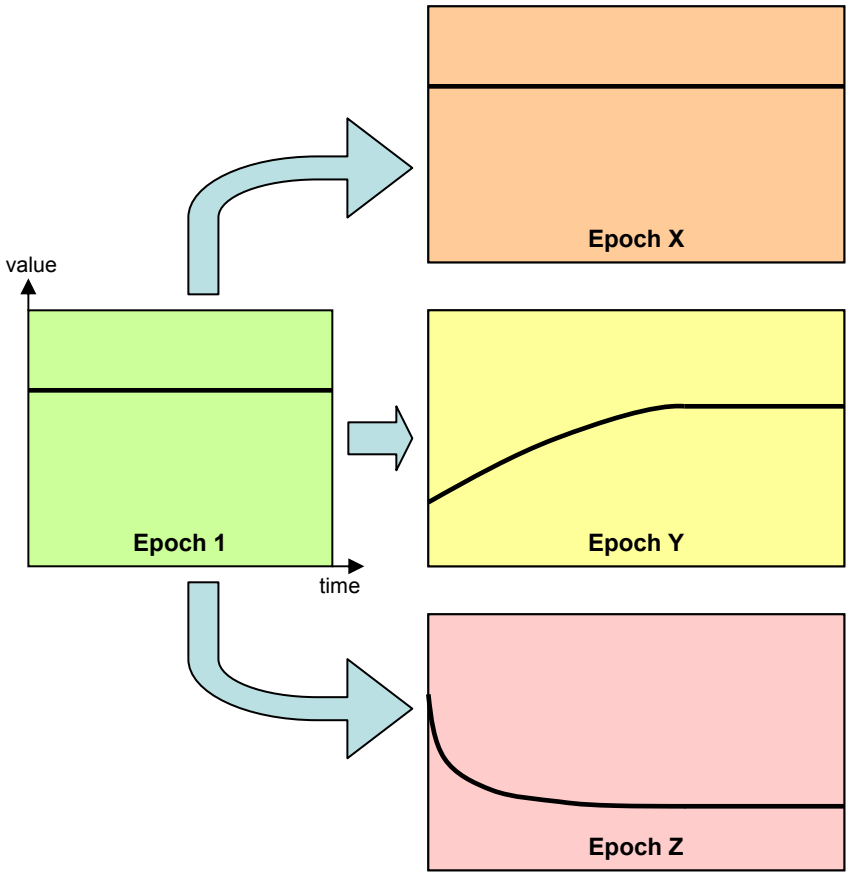
Time period during with a fixed context; characterized by static constraints, design concepts, available technologies, and articulated attributes (Ross 2006)

© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology

# How is this different from robustness?

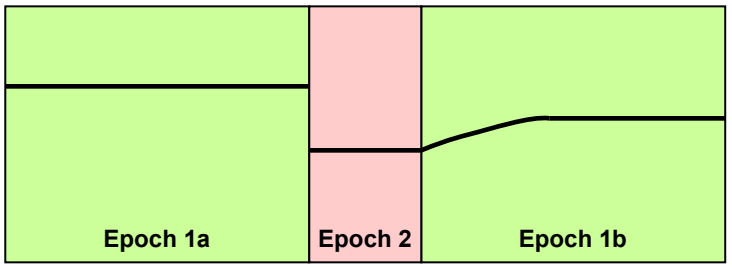
## Robust

Accommodating a permanent change in context




## Survivable

Recovers from a finite change in context




$$\underline{U}_{1a} = \begin{bmatrix} U_1 \\ U_2 \\ U_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$$

$U_2 \rightarrow 0$

$$\underline{U}_2 = \begin{bmatrix} 1 \\ 0 \\ 3 \end{bmatrix}$$

$$\underline{U}_{1b,start} = \begin{bmatrix} 1 \\ 0 \\ 3 \end{bmatrix}$$

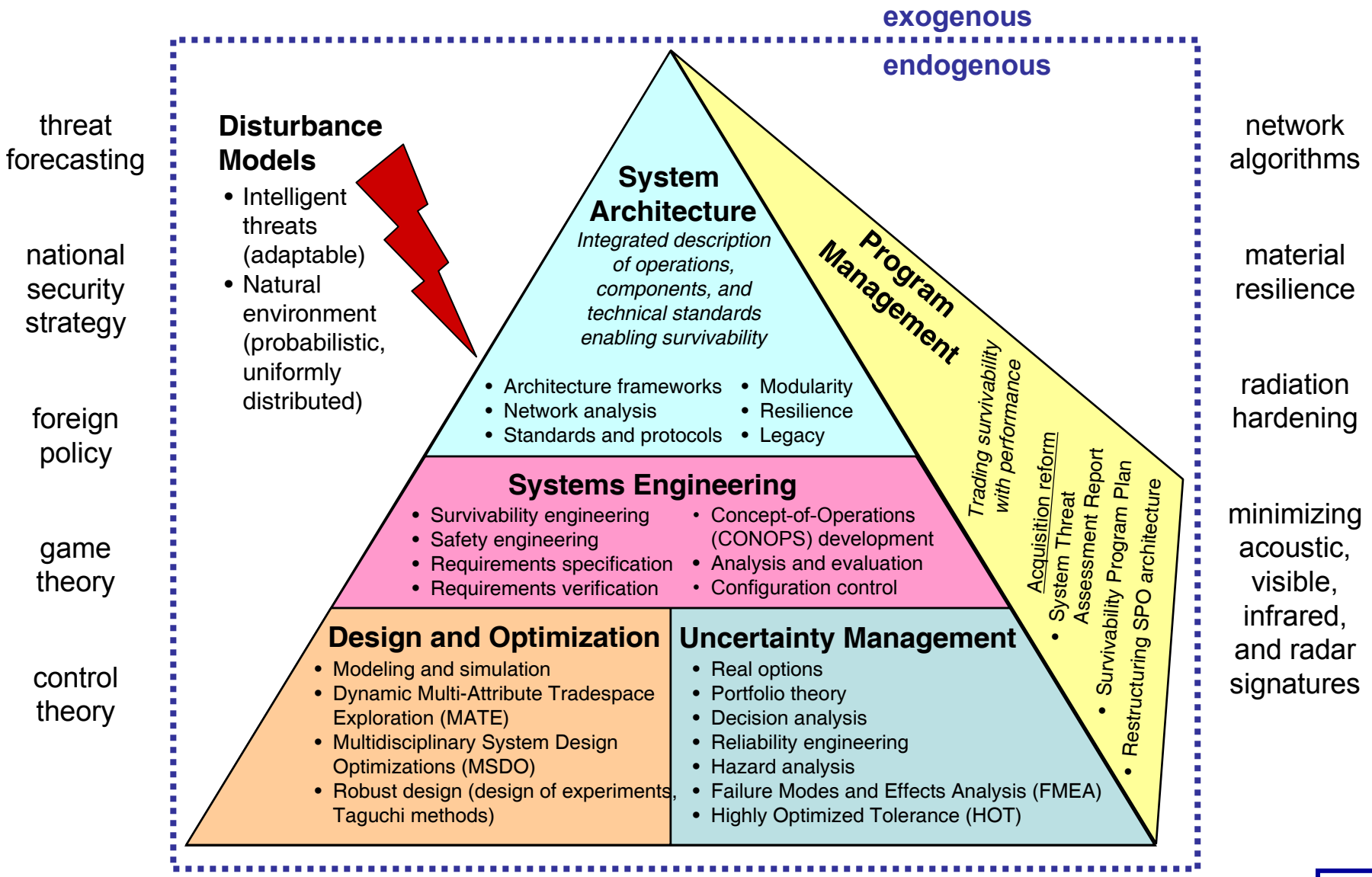
partial recovery

$$\underline{U}_{1b,end} = \begin{bmatrix} 1 \\ 1 \\ 3 \end{bmatrix}$$

Survivability and robustness are related yet distinct. Survivability is a special case of value robustness with a finite condition on disturbance duration.

© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology

# Relevant Disciplines




© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology

# Research Design

| 1. Knowledge Capture and Synthesis (Descriptive) | 2. Theory Development (Normative) | 3. Computer Experiments (1-2 Mapping) | 4. Case Applications (Prescriptive) |
|---|---|---|---|
| a) Literature review<br>b) Survivability definition<br>c) Survey & structured interviews<br>d) Descriptive case studies for each component of preliminary framework (functional view)<br>– Disturbance mechanism<br>• Terrorism<br>– Detection mechanism<br>• Space Situational Awareness (SSA)<br>– Decision mechanism<br>• National Command Authorities<br>– Response mechanism<br>• Nuclear "Triad" | Hypotheses<br>Framework<br>Metrics<br>Heuristics | Sensitivity analysis on various SSA network topologies<br>Space tug survivability to orbital debris (hardening & maneuverability) | Responsive space paradigm (e.g., Air Force TACSAT program)<br>Critical infrastructure protection (Homeland Security) |
| *Fall 2006 – Fall 2007* | *Winter 2006 →* | *Spring 2007 →* | *Spring 2008 →* |

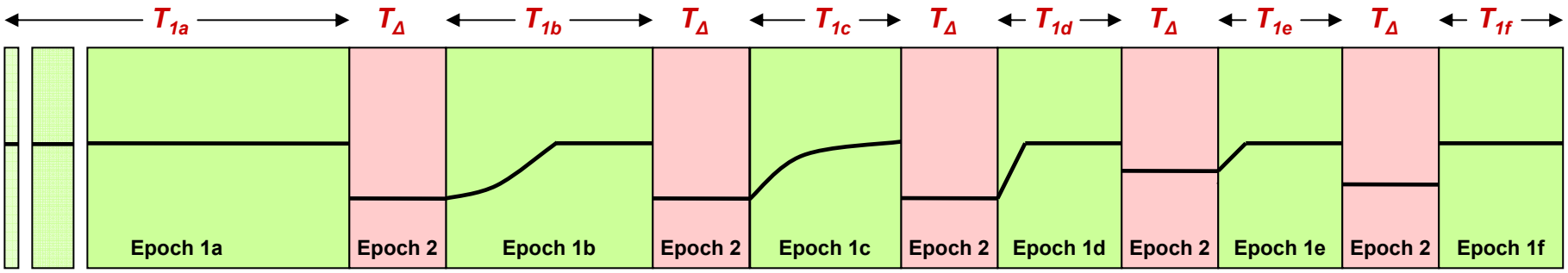
© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology

# Backup Slides

© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology

# Continuum Between Survivability and Robustness

*At what point do repeated disturbances constitute a change in context?*




**Survivable** ← impulse event — attack — disaster – market shift – policy change → **Robust**

when $\frac{T_\Delta}{T_1} << 1$

then *design for survivability*

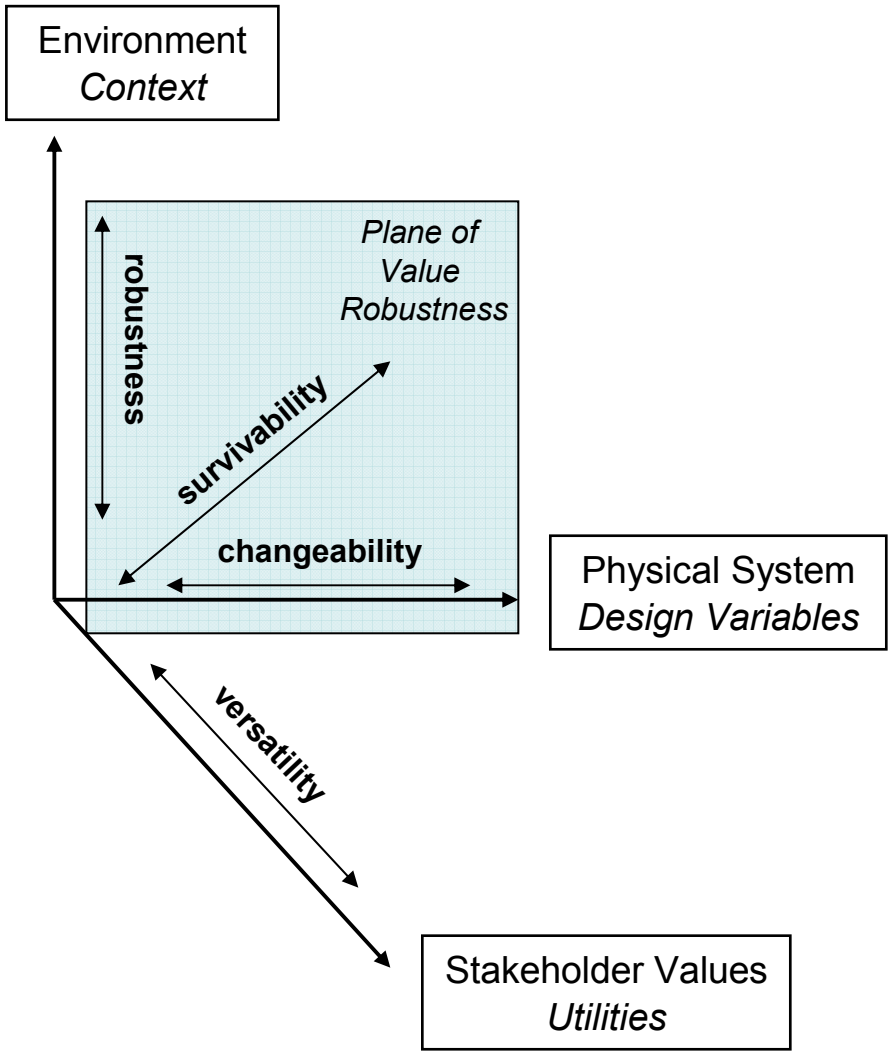
when the disturbance interval goes to 0…

$$\lim_{T_1 \to 0} environment \rightarrow epoch_{new}$$

then *design for robustness*

© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology

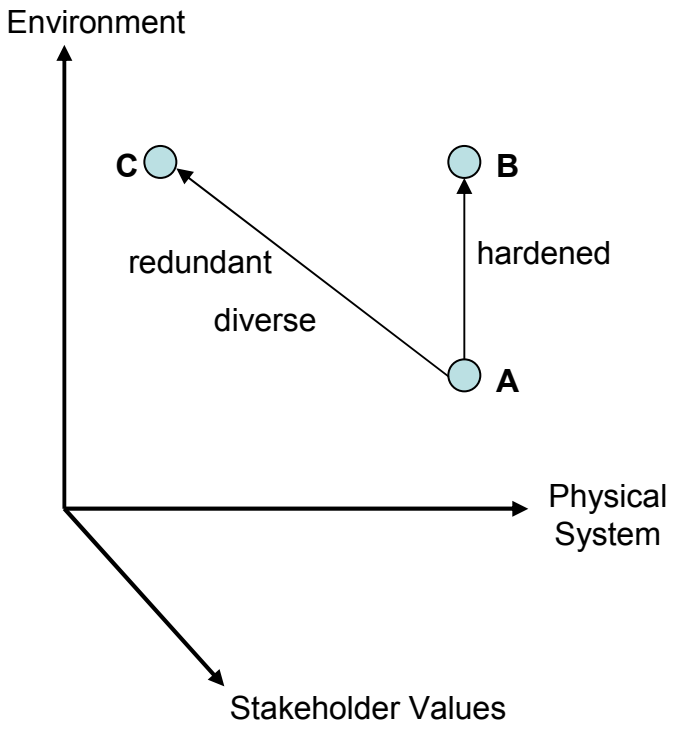
# Conceptual Frame: "Ility Space"

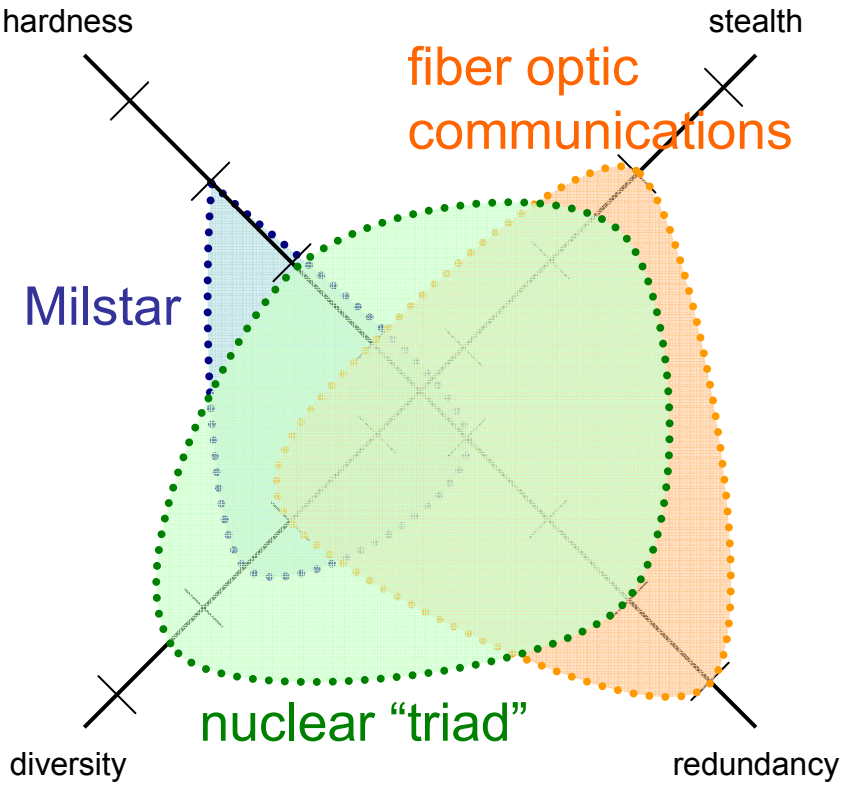



- Three sources of change for system
  - Constraints
  - Design Variables
  - Utilities
- Survivability may be considered a meta-framework for robustness and changeability
  - Passive Survivability
    - Ability of system to maintain value despite environmental disturbances
    - Special case of robustness
  - Active Survivability
    - Ability of system to react to environmental disturbances by modifying design variables
    - Special case of changeability
- Most systems incorporate both

© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology

# Passive Survivability



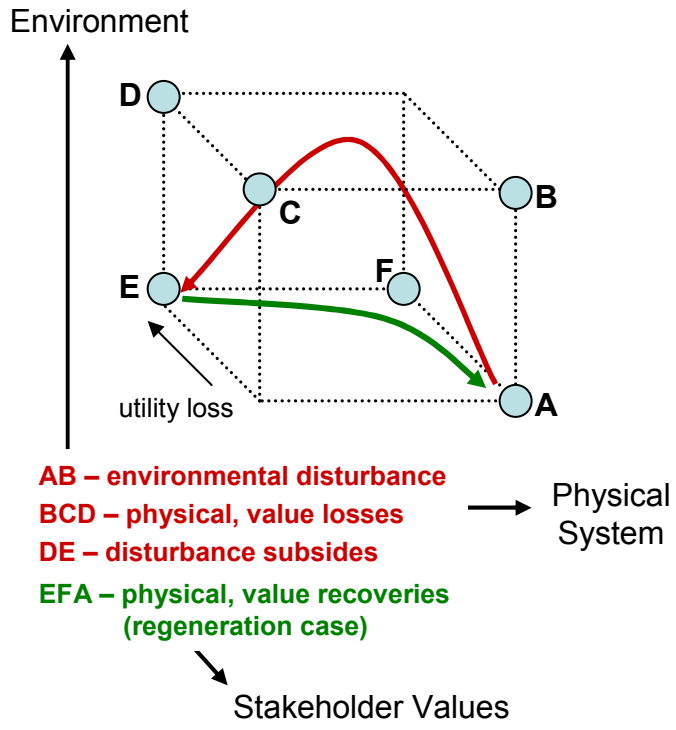



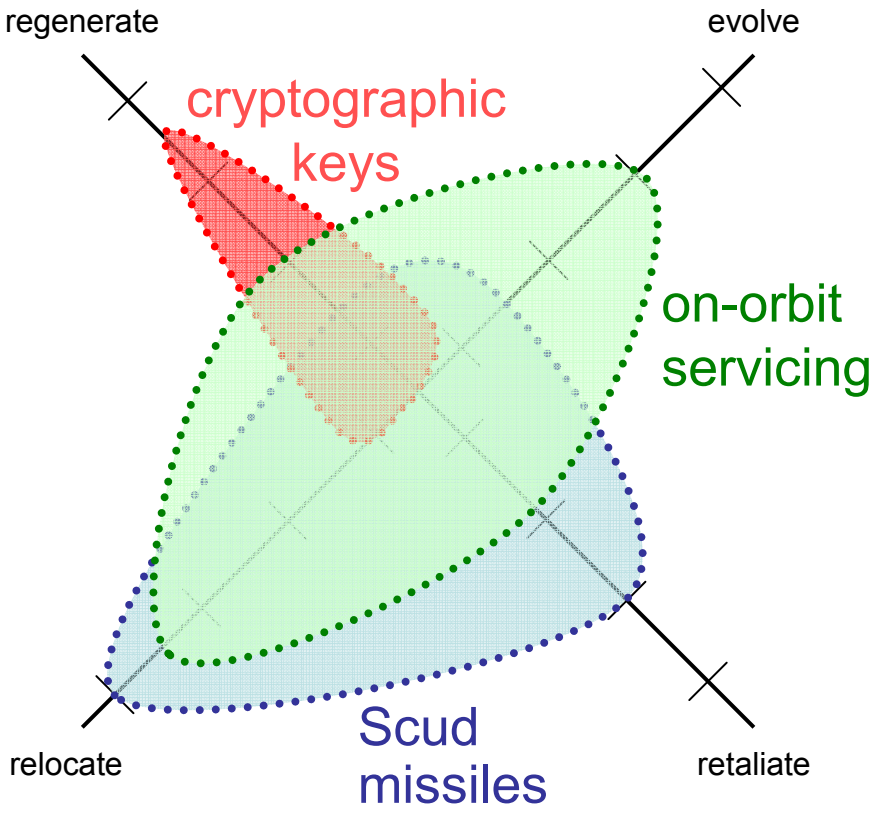

*4 design principles*

| | |
|---|---|
| hardness | resistance of a system to deformation; increased cost to attacker |
| stealth | ability of a system to conceal itself within its operating environment |
| redundancy | duplication of critical system components to increase reliability |
| diversity | variation in the range of systems within an architecture; mitigates HOT |

© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology

# Active Survivability




*4 design principles*

| | |
|---|---|
| regenerate | restoration of capability through repair and replacement activities |
| evolve | system modification to maintain and possibly extend capability |
| relocate | movement in position |
| retaliate | provision of negative consequences to origin of disturbance (deterrence) |

© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology

# Passive vs. Active Survivability

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

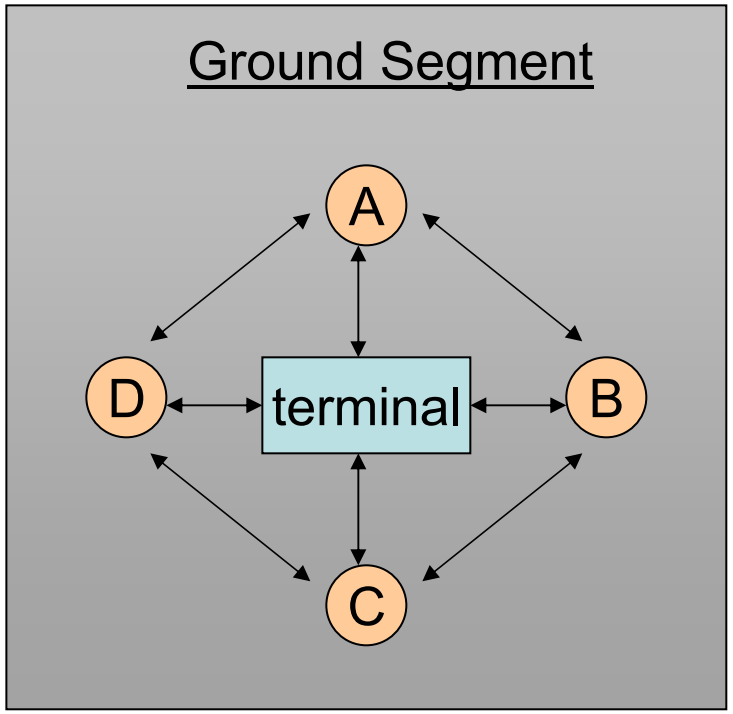
© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology

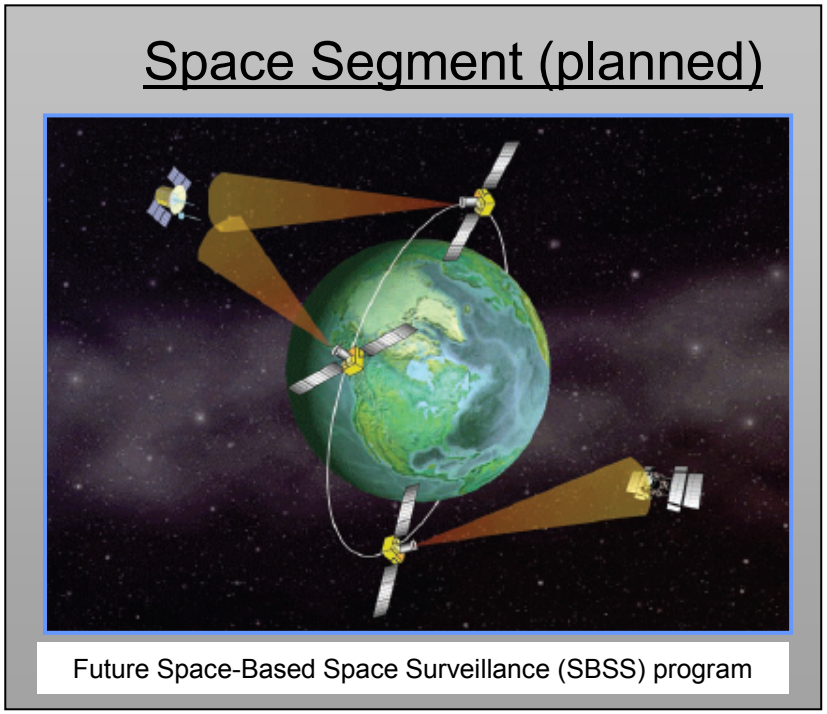
# Preliminary Hypotheses

- Design for survivability includes passive and active techniques
  - Each technique may be characterized by ~4 design principles
- Survivability is a special case of robustness
- Design for survivability involves trades between component-level, system-level, and architectural-level hardening
  - As disturbance threshold increases, there are diminishing returns associated with hardening individual components and systems
  - There are “tipping points” in the disturbance environment at which cost-effectiveness drives survivability to be addressed at higher levels in the architecture
  - A survivable architecture may be an emergent property of a network, requiring no hardening in the traditional sense (*i.e.,* of components and systems)
- Passive and active survivability are complementary goods

© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology

# Computer Experiment #1: Space Situational Awareness



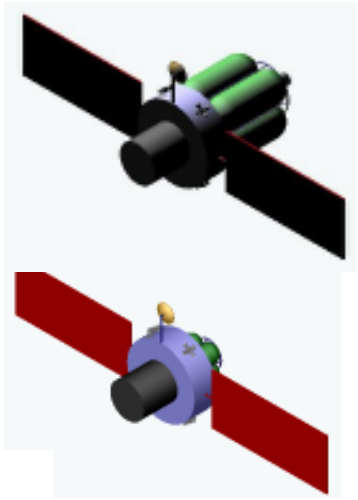



- What is the nature and type of coupling between SSA sensors?
- Which network topologies are more robust to environmental disturbances?
- How should designers trade-off between passive (*e.g.,* node hardening) and active (*e.g.,* flexible routing) survivability techniques?

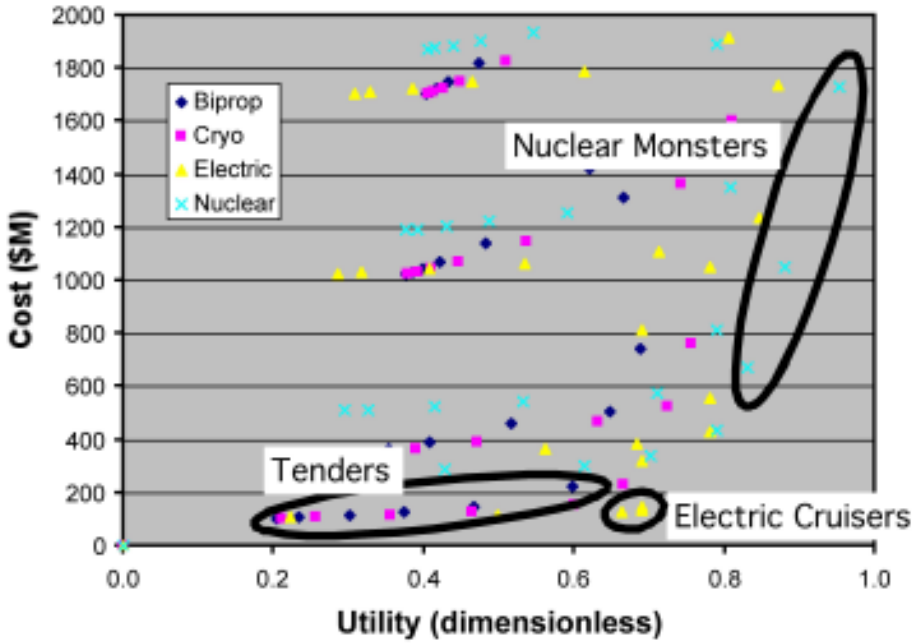
© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology

# Computer Experiment #2 – Space Tug

- Existing MATE study of space tug trade space
  - Three attributes
    - Delta-V
    - Capability
    - Response time
  - Three design variables



**Design Space**
- Manipulator Mass
  - Low (300kg)
  - Medium (1000kg)
  - High (3000 kg)
  - Extreme (5000 kg)
- Propulsion Type
  - Storable bi-prop
  - Cryogenic bi-prop
  - Electric (NSTAR)
  - Nuclear Thermal
- Fuel Load - 8 levels




- New MATE study incorporates survivability
  - Consider debris / kinetic kill vehicle (KKV)
  - Additional design variables
    - Hardening
    - Avoidance
  - Challenge: present "ility" with cost-utility tradespace

© 2007 Matt Richards, Engineering Systems Division, Massachusetts Institute of Technology