Architecting Systems for Value Robustness and Survivability

October 30, 2007

BAE Systems Executive Briefing at MIT

Dr. Donna H. Rhodes
rhodes@mit.edu

Dr. Adam M. Ross
adamross@mit.edu

Massachusetts Institute of Technology
Engineering Systems Division

MIT Engineering Systems Division as Intellectual Home for Advanced SE Research

SYSTEMS ENGINEERING (Traditional)

Systems engineering is the process of selecting and synthesizing the application of the appropriate scientific and technical knowledge in order to translate system requirements into system design. (Chase)

SYSTEMS ENGINEERING (Advanced)

Systems engineering is a branch of engineering that concentrates on design and application of the whole as distinct from the parts… looking at the problem in its entirety, taking into account all the facets and variables and relating the social to the technical aspects. (Ramo)

ENGINEERING SYSTEMS

A field of study taking an integrative holistic view of large-scale, complex, technologically-enabled systems with significant enterprise level interactions and socio-technical interfaces.

© 2007 Massachusetts Institute of Technology

Engineering Systems Requires Four Perspectives

1. A very **broad interdisciplinary perspective**, embracing technology, policy, management science, and social science.

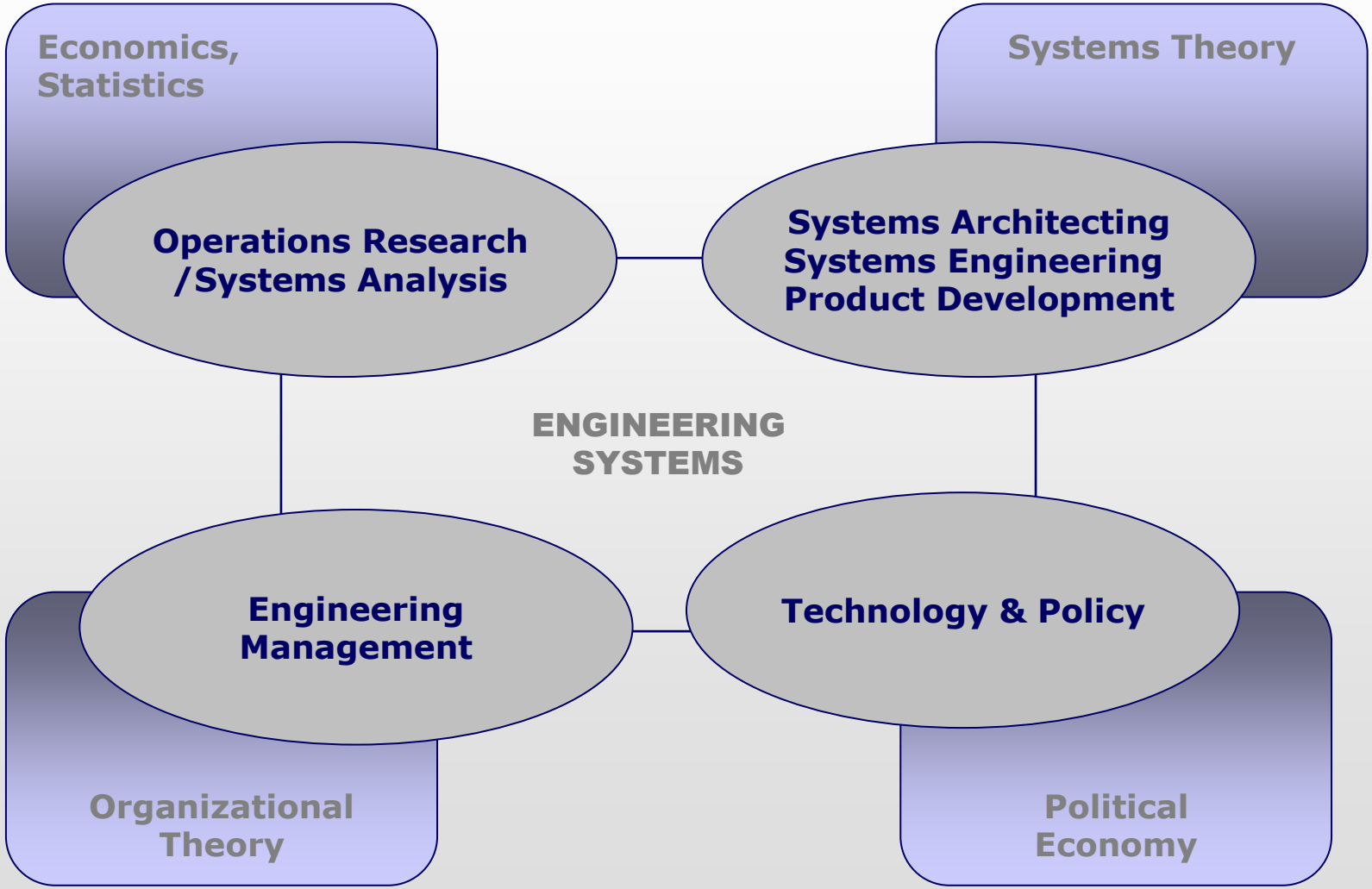
2. An **intensified incorporation of system properties** (such as sustainability, safety and flexibility) in the design process.
   - Note that these are lifecycle properties rather than first use properties.
   - These properties, often called “ilities” emphasize important intellectual considerations associated with long term use of engineering systems.

3. **Enterprise perspective**, acknowledging interconnectedness of product system with enterprise system that develops and sustains it.
   - This involves understanding, architecting and developing organizational structures, policy system, processes, knowledgebase, and enabling technologies as part of the overall engineering system.

4. A **complex synthesis of stakeholder perspectives**, of which there may be conflicting and competing needs which must be resolved to serve the highest order system (system-of-system) need.

© 2007 Massachusetts Institute of Technology

Engineering Systems as a Field of Study



© 2007 Massachusetts Institute of Technology

Changing Face of Systems Engineering

TRADITIONAL SE

Transformation of customer requirements to design

Requirements clearly specified, frozen early

Emphasis on minimizing changes

Design to meet well specified set of requirements

Performance objectives specified at project start

Focus on reliability, maintainability, and availability

ADVANCED SE

Effective transformation of stakeholder needs to fielded (and sustainable) solution

Focus on **product families and systems-of-systems**

Complex **interdependencies of system and enterprise**

Growing importance of **systems architecting**

Designing to accommodate change

Emphasis on **expanded set of "ilities"** and designing in *robustness, flexibility, adaptability* in concept phase

© 2007 Massachusetts Institute of Technology

DSB/AFSAB Report on Acquisition of National Security Space Programs

May 2003

Findings:

Cost has replaced mission success as the primary driver in managing space development programs

Unrealistic estimates lead to unrealistic budgets and unexecutable programs

Undisciplined definition and uncontrolled growth in system requirements increase cost and schedule delays

Government capabilities to lead and manage the acquisition process have seriously eroded

Industry has failed to implement proven practices on some programs

© 2007 Massachusetts Institute of Technology

LAI/AF Systems Engineering for Robustness Workshop

Washington, DC in June 2004

- According to Dr. Marvin Sambur, "Systems Engineering for Robustness" means developing systems that are…

  - Capable of *adapting* to changes in mission and requirements
  - *Expandable/scalable*, and designed to accommodate growth in capability
  - Able to *reliably* function given changes in threats and environment
  - Effectively/affordably *sustainable* over their lifecycle
  - Developed using products designed for use in various *platforms* and systems
  - Easily *modified* to leverage new technologies

- "Robustness" scope expanded beyond classical robustness …
- Experts questioned…
  - What does it mean?
  - How can it be measured/analyzed?
  - Who is going to pay for it?

How can designers account for this new "robustness"?

*Adapted from Ross, A., Rhodes, D., and Hastings, D., "*Defining System Changeability: Reconciling Flexibility, Adaptability, Scalability, and Robustness for Maintaining System Lifecycle Value*," INCOSE Int'l Symposium 2007, San Diego, CA, June 2007

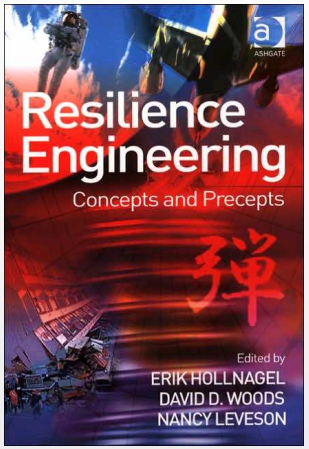
© 2007 Massachusetts Institute of Technology

Motivation – Resilience Engineering

Research Agenda for Systems of Systems (SoS) Architecting

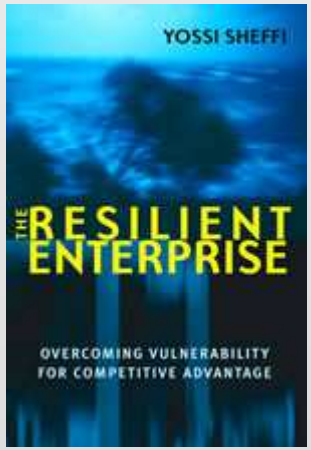
1. Resilience
2. Illustration of Success
3. System vs. SoS Attributes
4. Model Driven Architecting
5. Multiple SoS Architectural Views
6. Human Limits to Handling Complexity
7. Net-Centric Vulnerability
8. Evolution
9. Guided Emergence
10. No Single Owner SoS

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



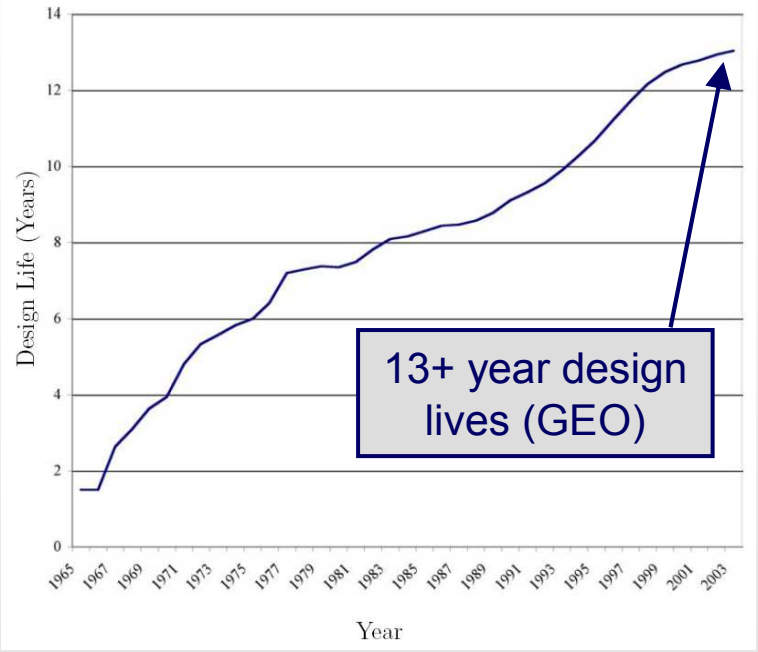
© 2007 Massachusetts Institute of Technology

Motivation – Environment

1960's Paradigm

- 30-45 day missions
- Example: 144 Corona spacecraft launched between 1959-1972

Current State

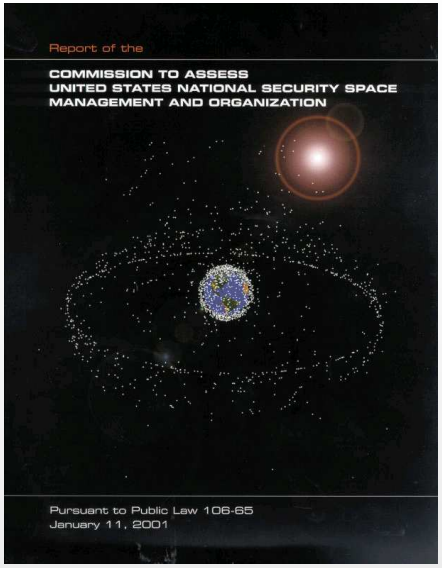


- Less agility to adapt to environmental uncertainties
- Dynamic technologies, markets, threats

Growth in satellite complexity and design life has bred fragility

© 2007 Massachusetts Institute of Technology

Motivation – National Studies



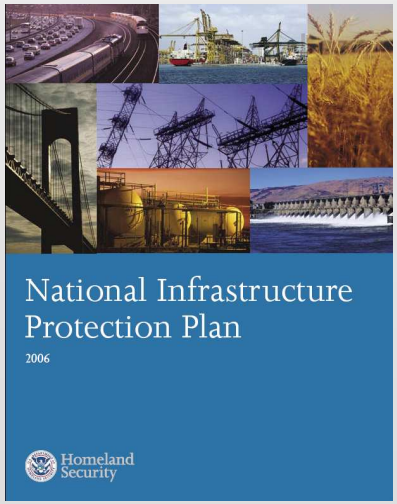
2001 Rumsfeld Space Commission

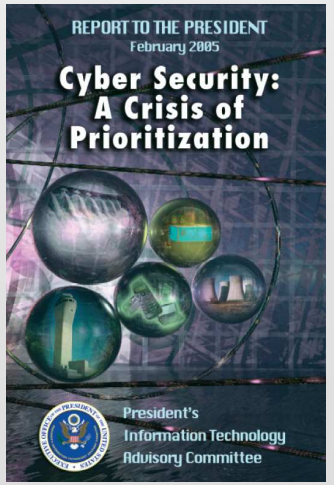
- Identified vulnerabilities of USG space assets due to:
  - Denial & Deception
  - Interference
  - Jamming
  - Microsatellites attacks
  - Nuclear detonation
- Discussed surprise attack as "Pearl Harbor in Space"
  - Vulnerability exacerbated by reliance on commercial systems
  - Inadequate Space Situational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

Motivation for New Research

As the interdependence of large-scale, distributed systems has grown, 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
- Conventional approaches to survivability
  - Focus on physical aspects
  - Presuppose environment and hazards
  - Ineffective for emergent and context-dependent properties

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

© 2007 Massachusetts Institute of Technology

Research Summary

Project Title: ***Architecting for Survivability: Conceptual Design of Aerospace Systems Robust to Finite Disturbances***

Research Assistant:

Matt Richards, ESD Doctoral Student, PhD expected '09

Sponsor:

National Science Foundation / Program on Emerging Technologies

Goal:

To improve aerospace system survivability by informing future acquisitions using a dynamic tradespace exploration framework for analyzing, quantifying, and specifying survivability

Approach:

- Extend dynamic Multi-Attribute Tradespace Exploration (MATE) methodology (Ross 2006) with metrics for survivability
- Simulate performance of different space architectures (e.g., current paradigm, ORS) in various disturbance environments

© 2007 Massachusetts Institute of Technology

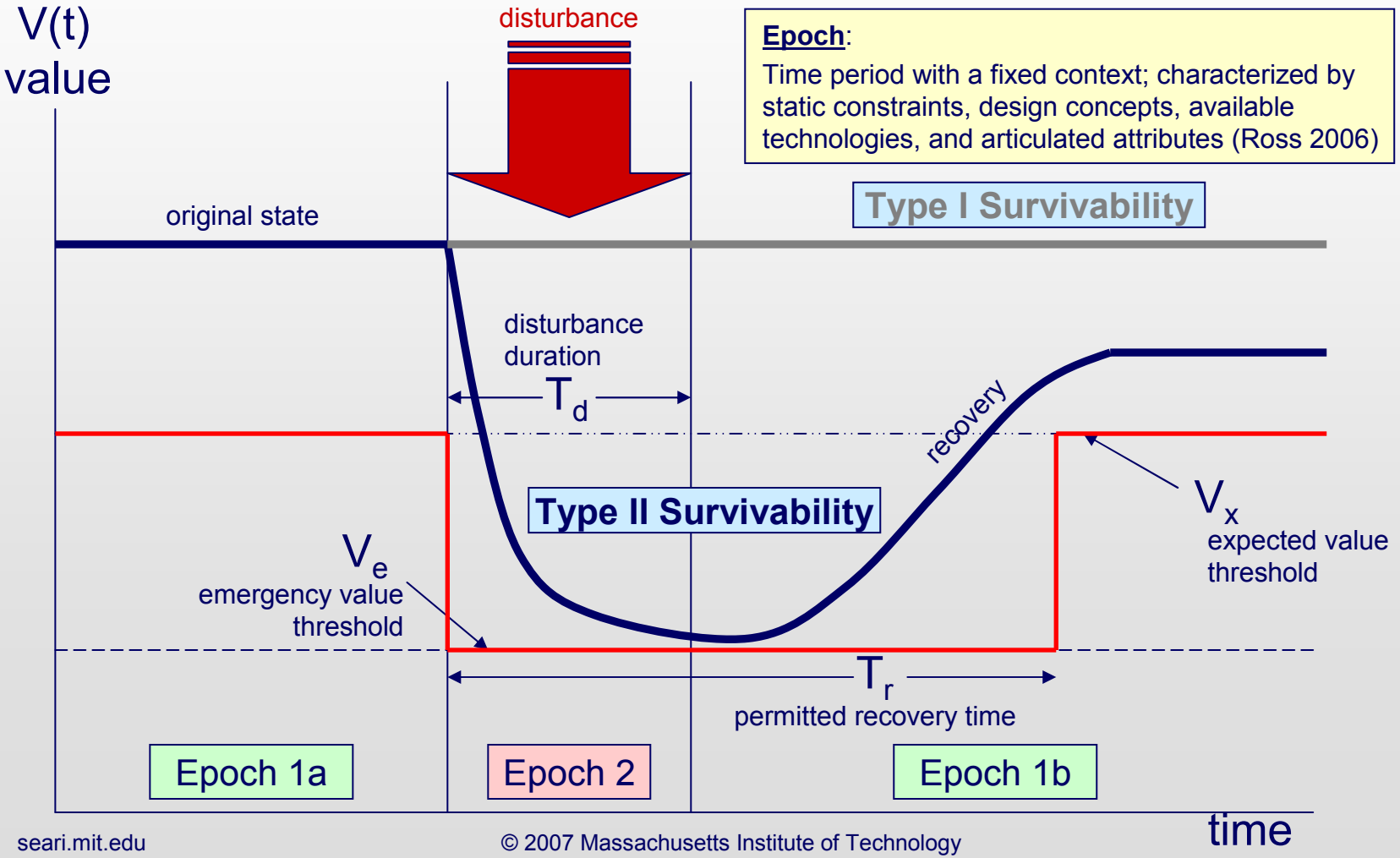
Key Challenges

- Incorporate “ilities” in front-end design activities
  - Identified need for systems to operate in the presence of change
  - How do we evaluate these elusive, ***temporal system properties***?
- Explore implications of low-probability, high-consequence events for value delivery
  - Asymmetric returns associated with designing for survivability
  - ***Diversity in risk tolerance*** across stakeholders of a given architecture
- Address implementation challenges associated with modifying existing infrastructures
  - Align ***incremental***, local decision-making
  - Leverage ***legacy*** architecture
  - Meet ongoing ***availability*** requirements

© 2007 Massachusetts Institute of Technology

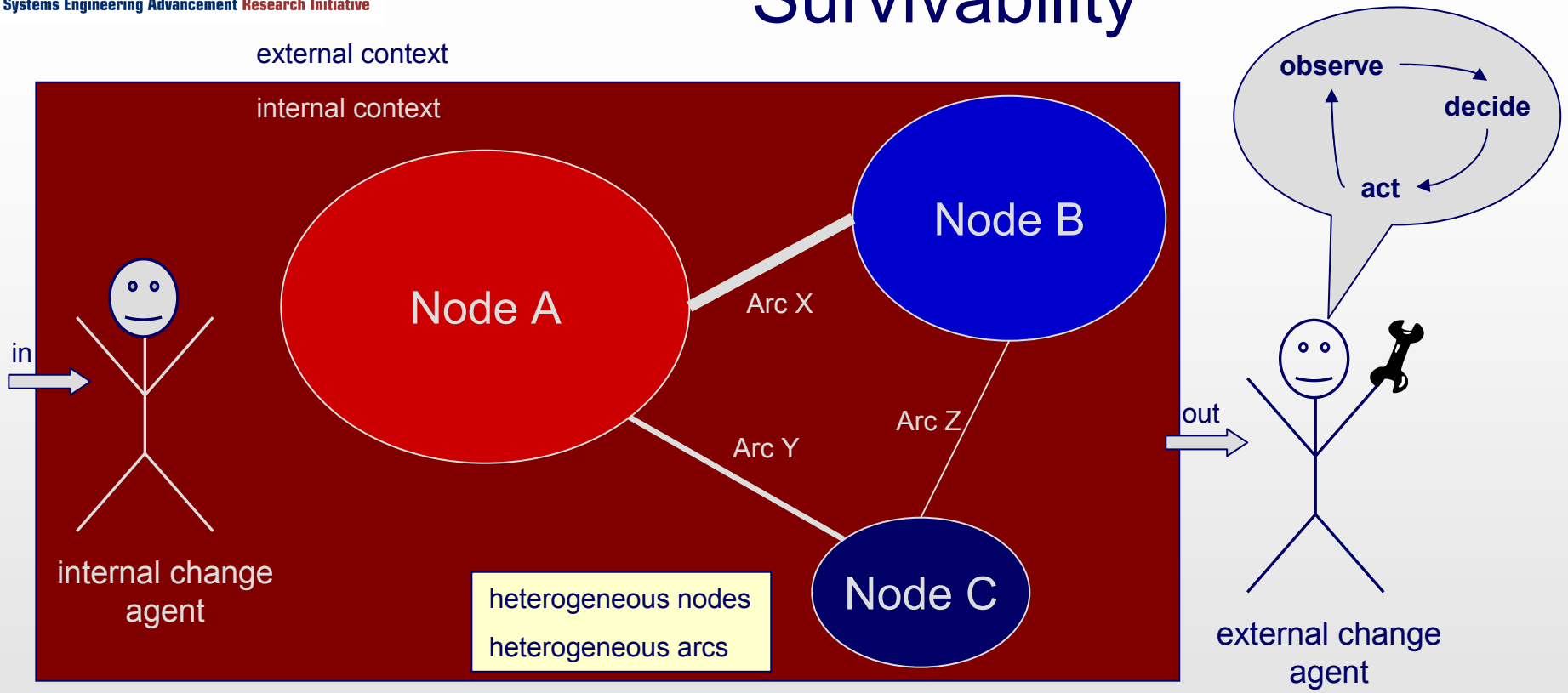
Definition of Survivability

Ability of a system to minimize the impact of a finite disturbance on value delivery, achieved through either (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



© 2007 Massachusetts Institute of Technology

Theoretical Construct for Survivability



Construct consists of the minimum set of elements to describe system

- Changes in elements will provide insights into survivability
- Used to enumerate 12 design principles for survivability
  - 6 identified for Type 1 survivability *(reduction in susceptibility)*
  - 6 identified for Type 2 survivability *(reduction in vulnerability)*

© 2007 Massachusetts Institute of Technology

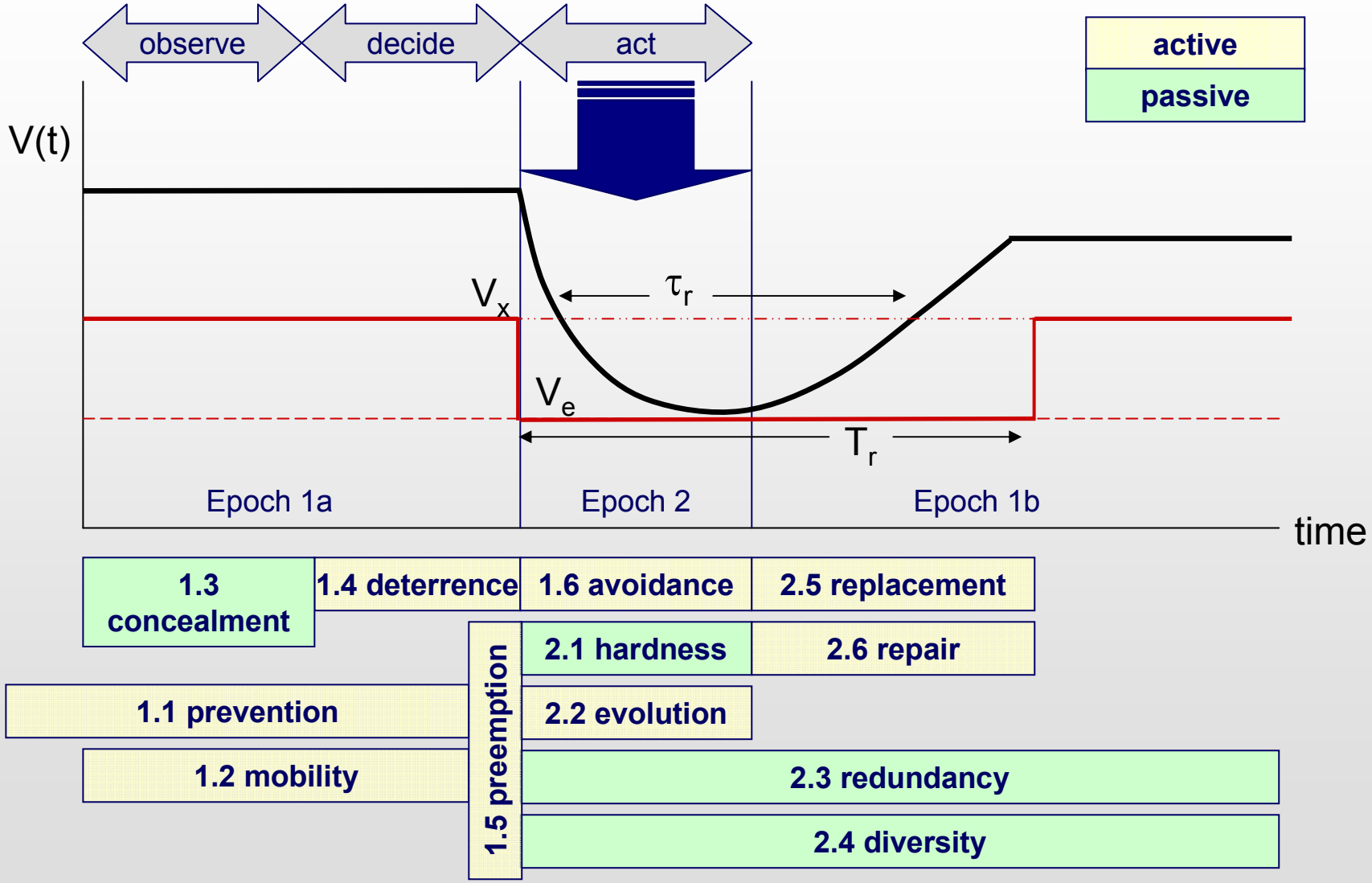
Design Principles of Survivability

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

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

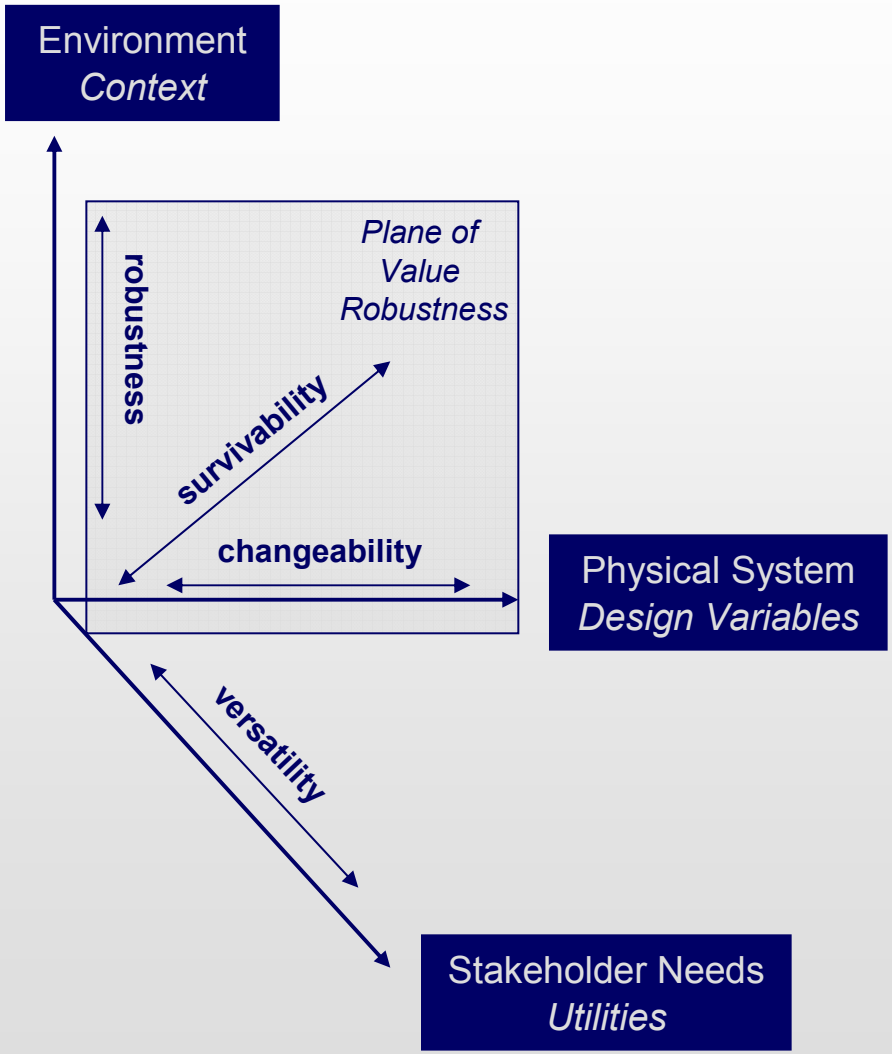
© 2007 Massachusetts Institute of Technology

Survivability Principles at Work



© 2007 Massachusetts Institute of Technology

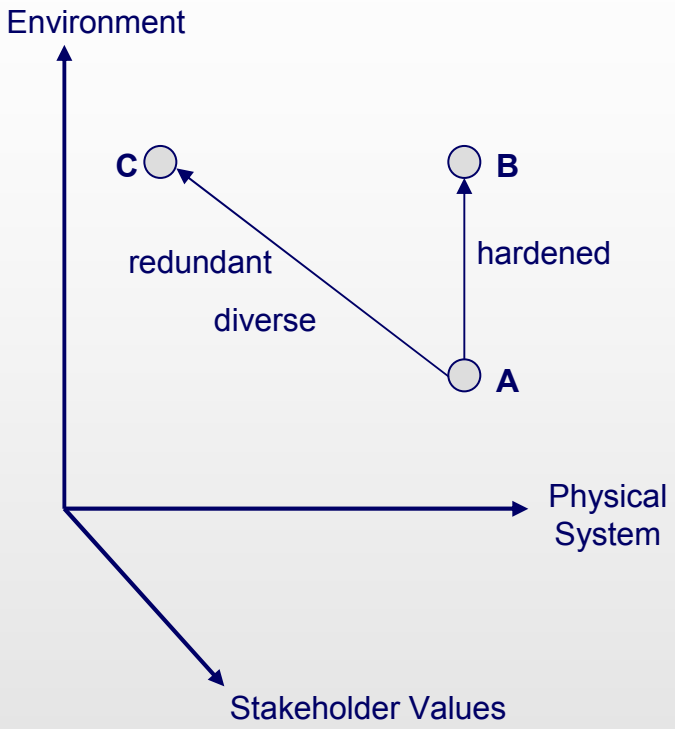
Conceptual Frame: "Ility Space"

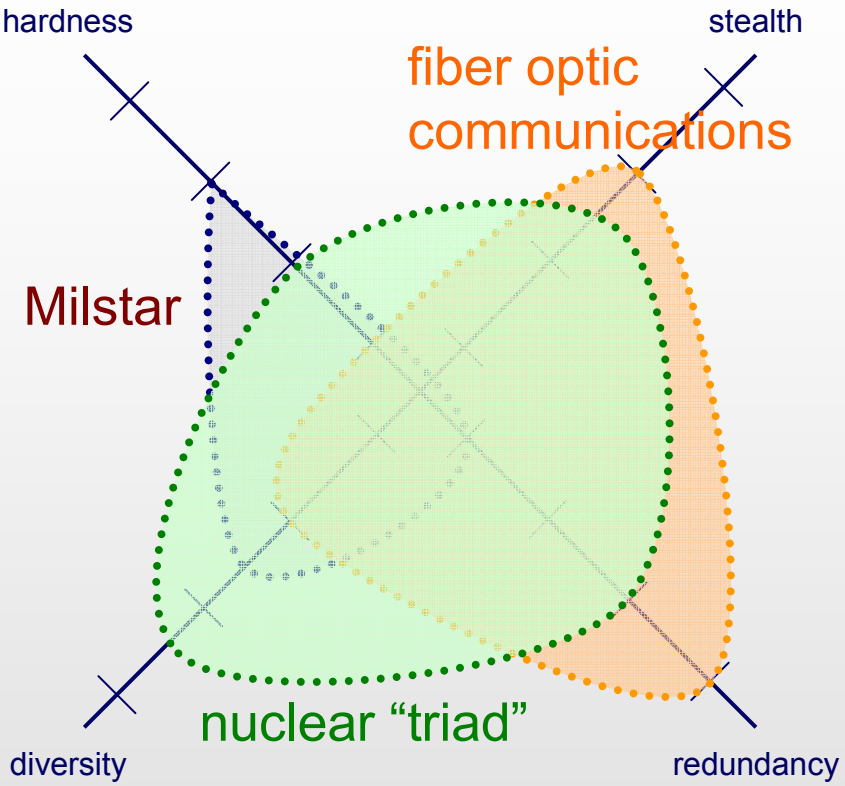


- Three axes of system change
  - Context
  - Design Variables
  - Utilities
- Survivability may be considered a meta-framework for robustness and changeability
  - Passive Survivability
    - Ability of system to maintain value despite environmental disturbances
    - Special case of robustness
  -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

© 2007 Massachusetts Institute of Technology

Passive Survivability



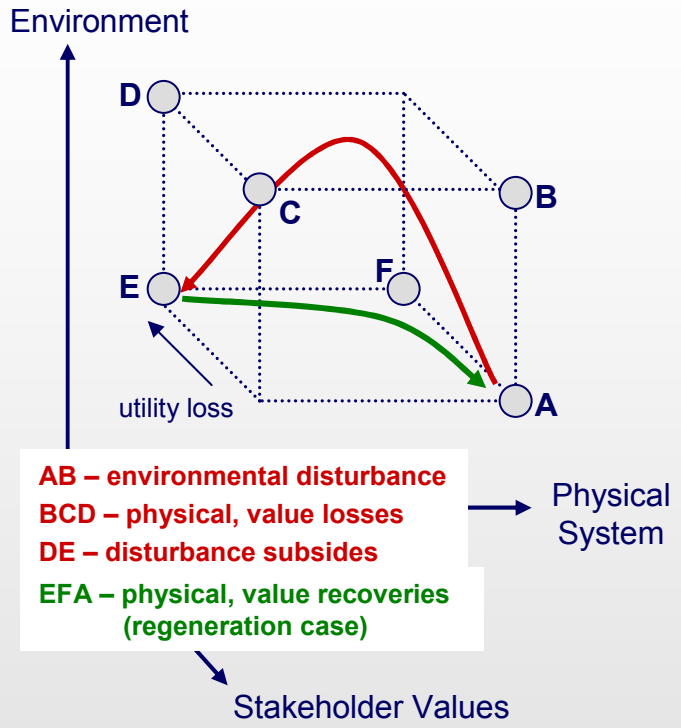


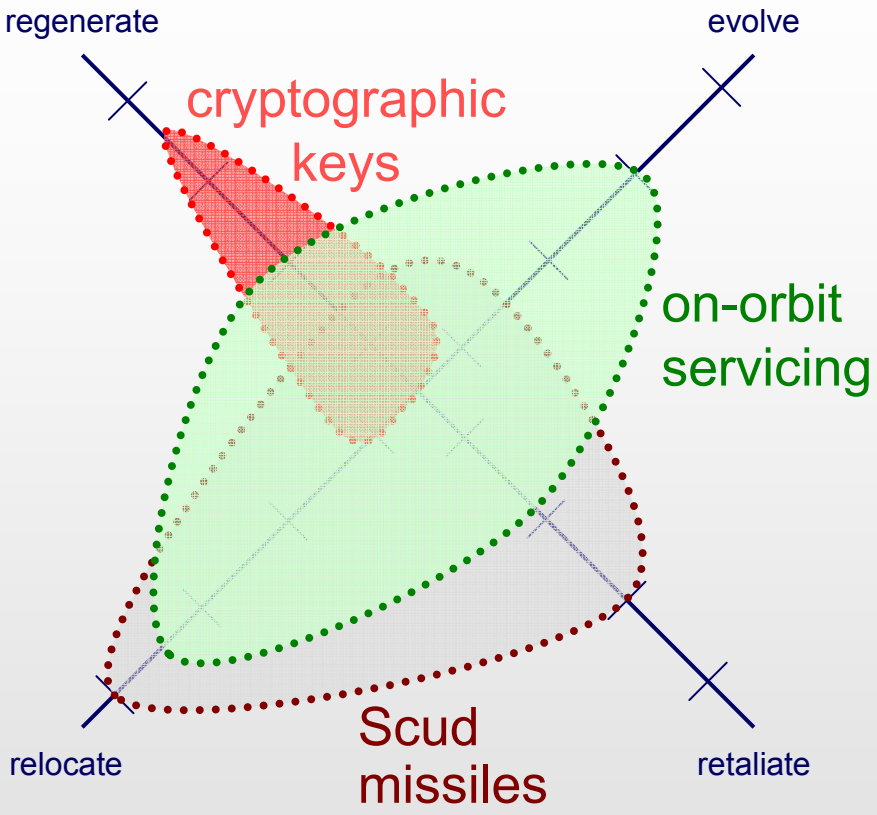
4 design principles

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 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 Massachusetts Institute of Technology

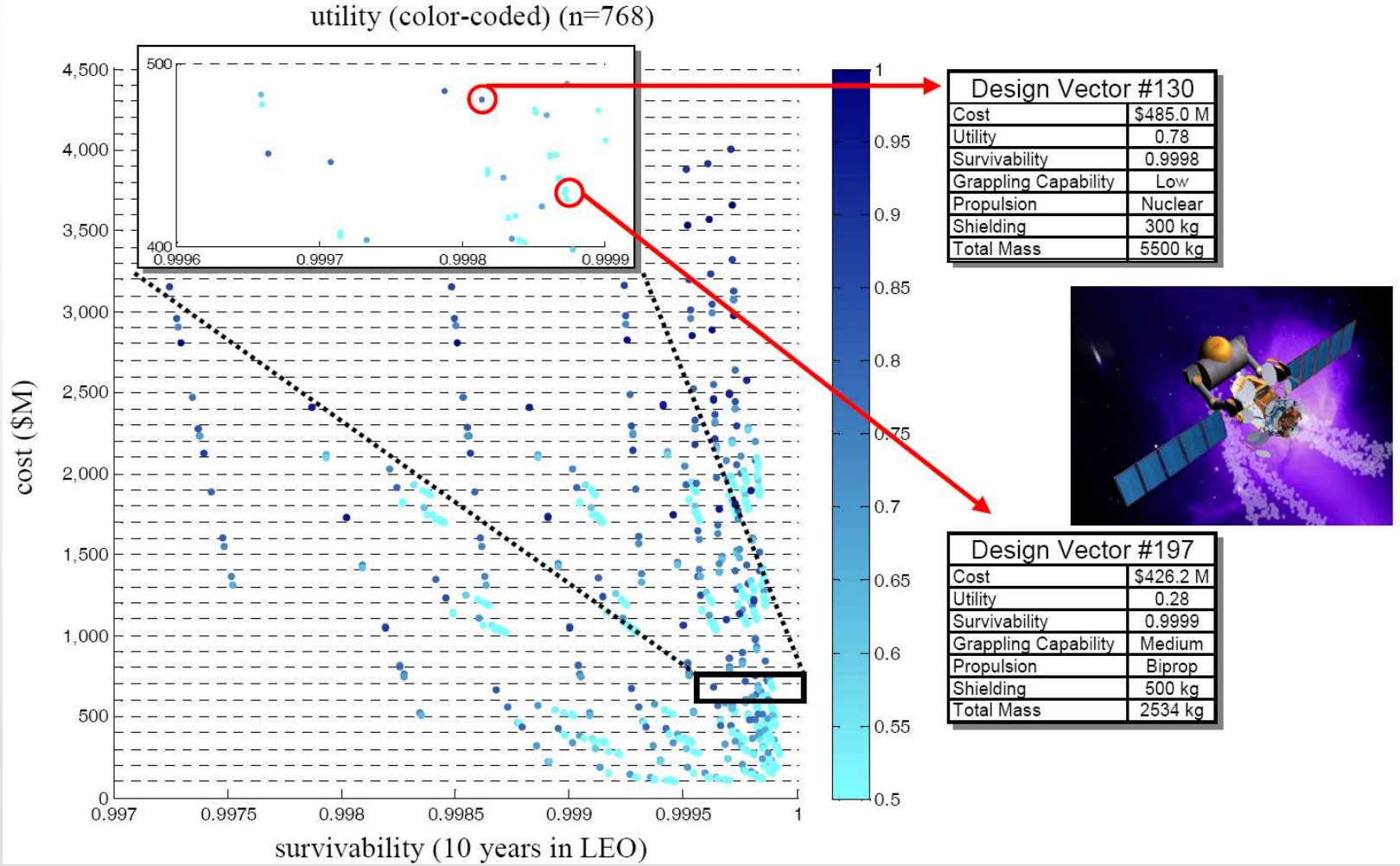
Challenge of Incorporating "ilities" in Tradespace Studies

- Temporal system properties that are difficult to represent in a static tradespace
- "ilities" (currently) need to be disaggregated from attributes
  - Attributes need to be independent, but…
  - "ilities" defined by attribute performance over time…
  - So "ilities" cannot be incorporated into attribute set or aggregated into a multi-attribute utility
- Abstract view of "ilities" represented in "ilities-space" difficult to implement in tradespace representations

*Adapted from McManus, H.M., Richards, M.G., Ross, A.M., and Hastings, D.E., "*A Framework for Incorporating "ilities" in Tradespace Studies*," AIAA Space 2007, Long Beach, CA, September 2007

© 2007 Massachusetts Institute of Technology

Sample Survivability Tradespace

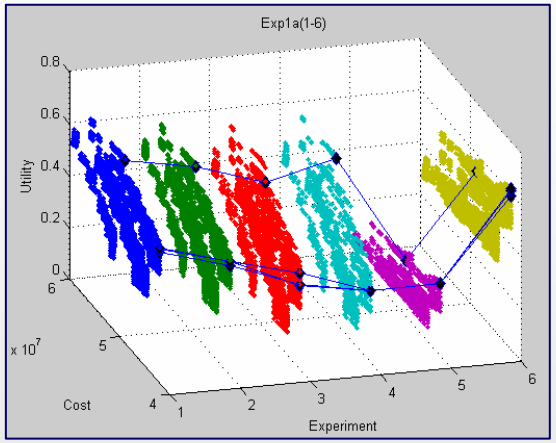


McManus, H., Richards, M., Ross, A., and Hastings, D., "A Framework for Incorporating "ilities" in Tradespace Studies," *AIAA Space 2007*, Long Beach, CA, September 2007.

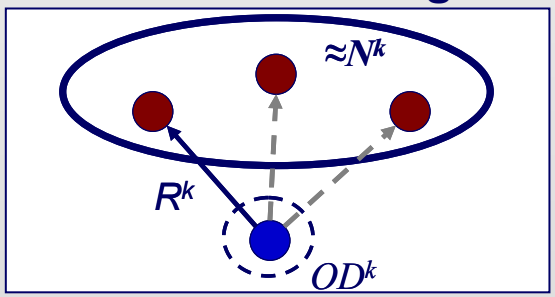
© 2007 Massachusetts Institute of Technology

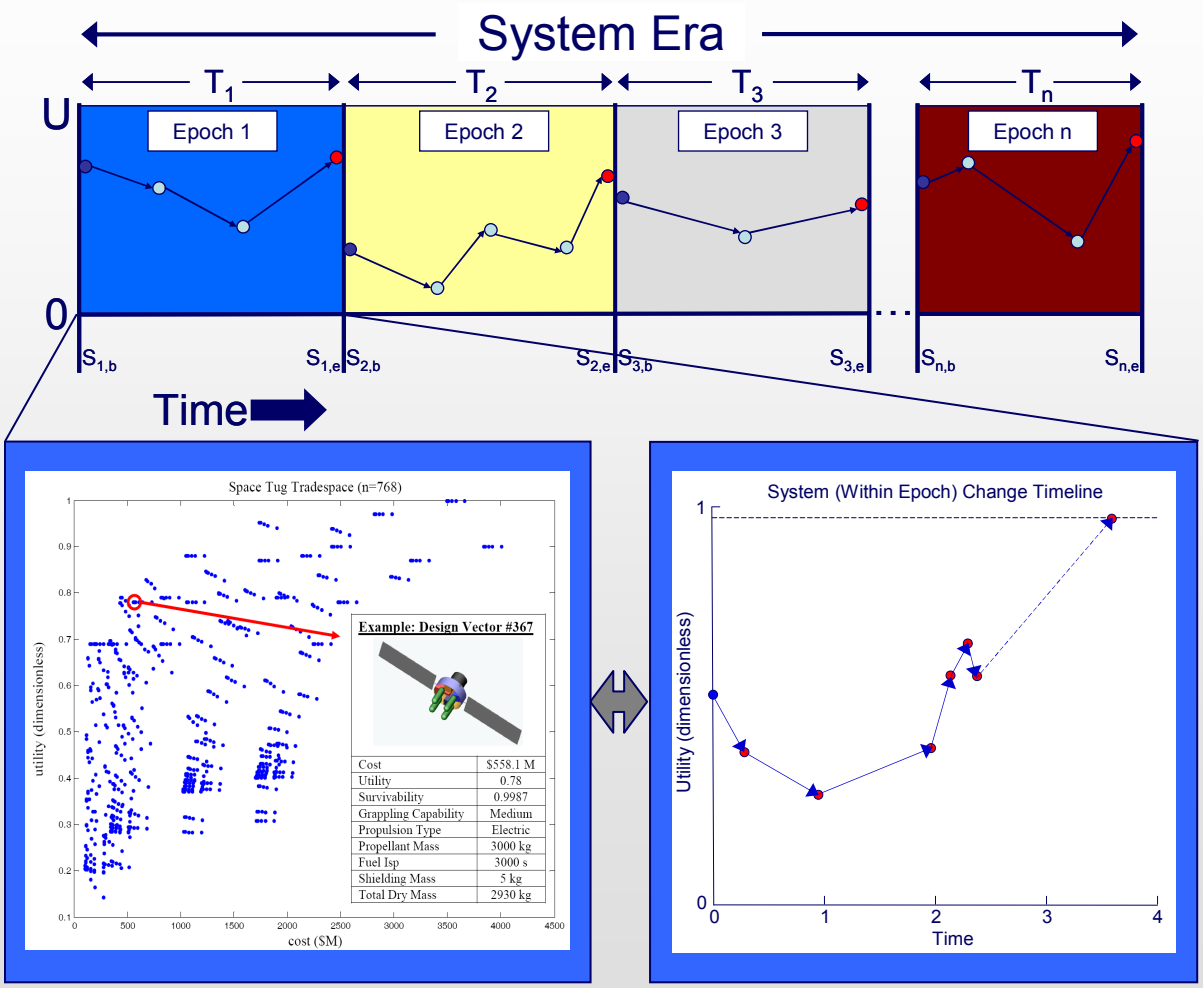
The System Era for Linking Tradespaces over Time

Pareto Tracing across Epochs



Changeability Quantified as Filtered Outdegree



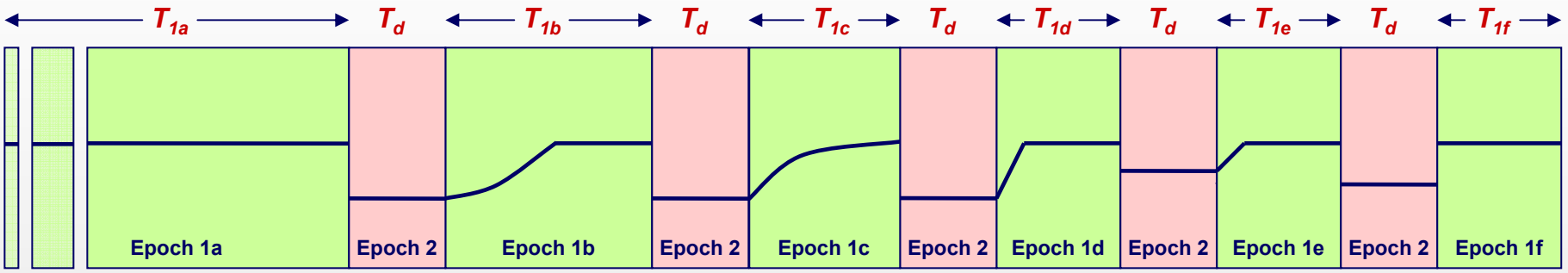


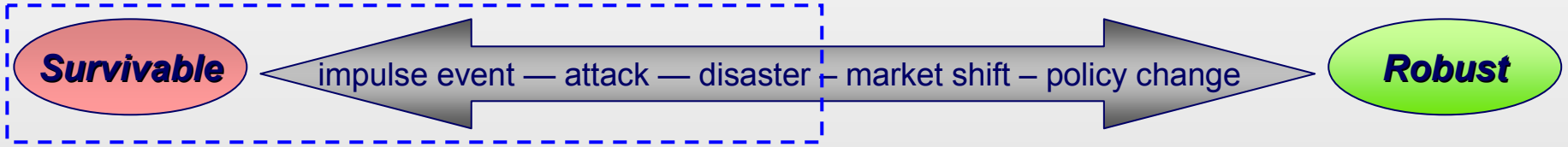
Temporal strategy can be developed across tradespaces within an Era

© 2007 Massachusetts Institute of Technology

Continuum Between Survivability and Robustness

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





when $\frac{T_d}{T_1} << 1$

then *design for survivability*

when the disturbance interval goes to 0…

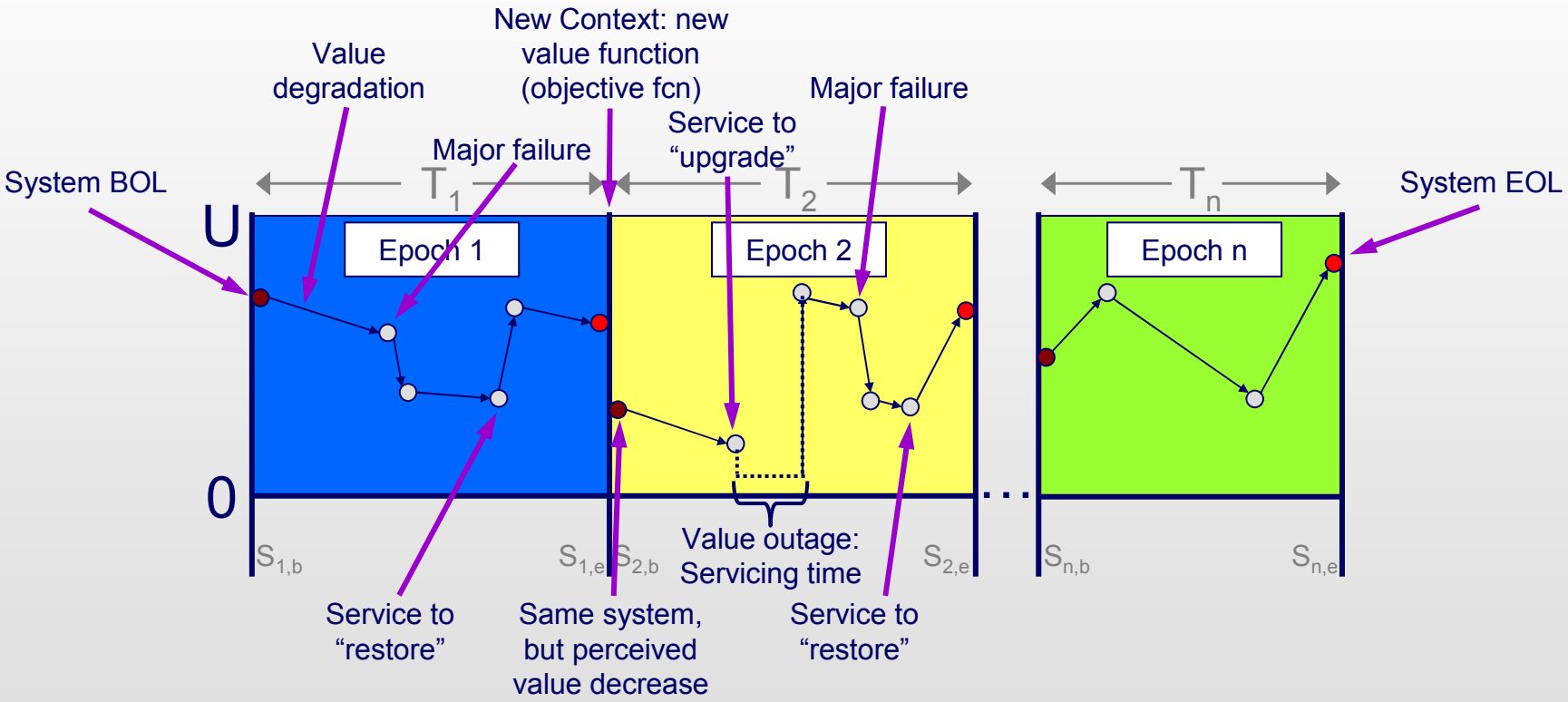
$$\lim_{T_1 \to 0} environment \to epoch_{new}$$

then *design for robustness*

© 2007 Massachusetts Institute of Technology

Example System Era

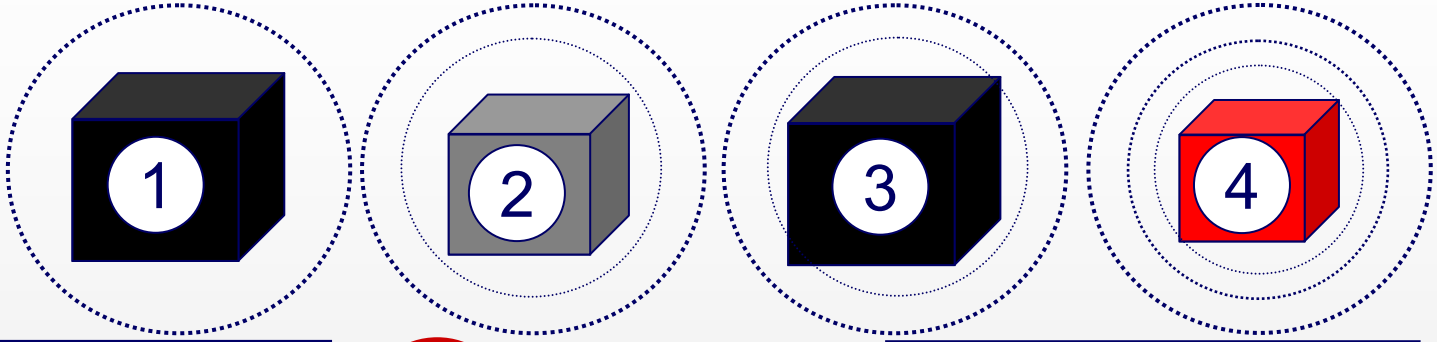
Example system: Serviceable satellite



System era with "serviceability"-enabled paths allow value delivery

© 2007 Massachusetts Institute of Technology

Ex: Desiring "No" Change:
Value Robustness



Preferences t=1

Attribute	k_i
Size	0.5
Loudness	0.2

Choose 3

U(3)>U(2)>U(1)>U(4)

U(4)>U(2)>U(3)>U(1)

big>small

loud>quiet

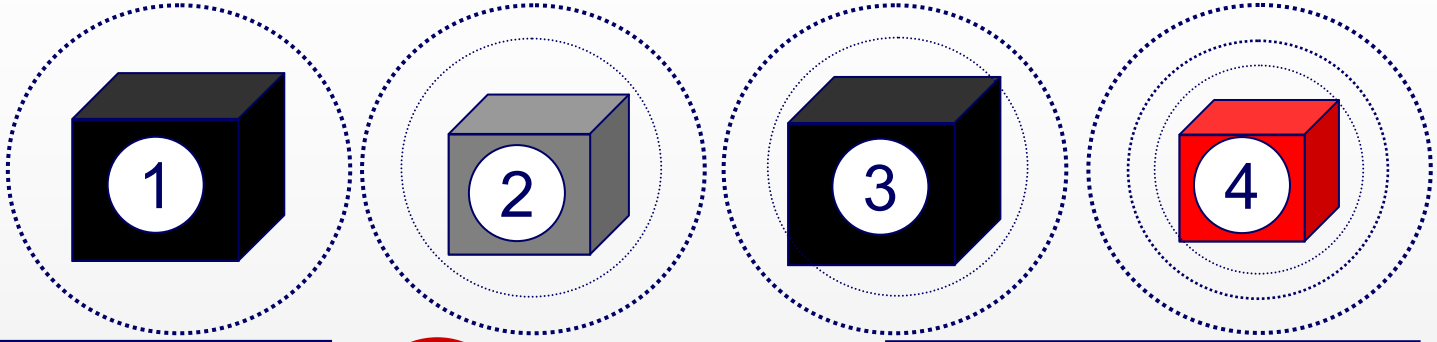
Preferences t=2

Attribute	k_i
Size	0.5
Loudness	0.2

Attribute "priority"

© 2007 Massachusetts Institute of Technology

Ex: Desiring "No" Change:
Value Robustness



Preferences t=1

Attribute	k_i
Size	0.5
Loudness	0.2

Choose 3

U(3)>U(2)>U(1)>U(4)

U(4)>U(2)>U(3)>U(1)

big>small

loud>quiet

red>gray>black

Preferences t=2

Attribute	k_i
Size	0.5
Loudness	0.2
Color	0.6

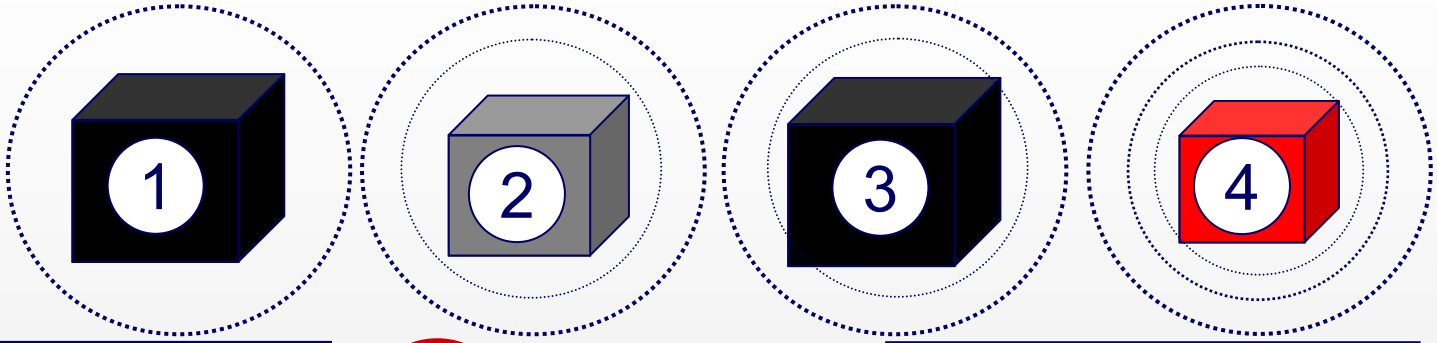
Attribute "priority"

New

Choose 4

© 2007 Massachusetts Institute of Technology

Ex: Desiring "No" Change:
Value Robustness



Preferences t=1

Attribute	k_i
Size	0.5
Loudness	0.2

Choose 3

U(3)>U(2)>U(1)>U(4)

U(4)>U(2)>U(3)>U(1)

big>small

loud>quiet

red>gray>black

Change?

Preferences t=2

Attribute	k_i
Size	0.5
Loudness	0.2
Color	0.6

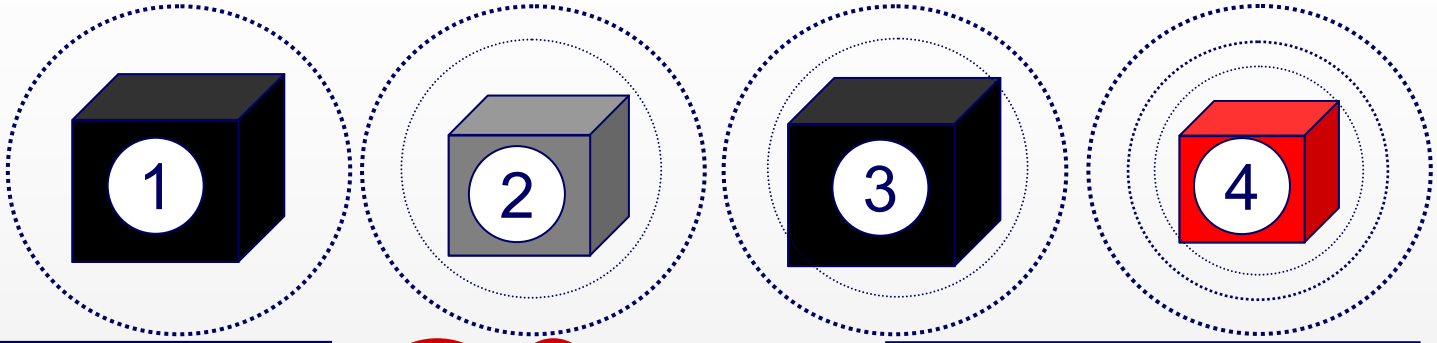
Attribute "priority"

New

Choose 4

© 2007 Massachusetts Institute of Technology

Ex: Desiring "No" Change:
Value Robustness



Preferences t=1

Attribute	k_i
Size	0.5
Loudness	0.2

Choose 3

U(3)>U(2)>U(1)>U(4)

U(4)>U(2)>U(3)>U(1)

big>small

loud>quiet

red>gray>black

Change?

Preferences t=2

Attribute	k_i
Size	0.5
Loudness	0.2
Color	0.6

Attribute "priority"

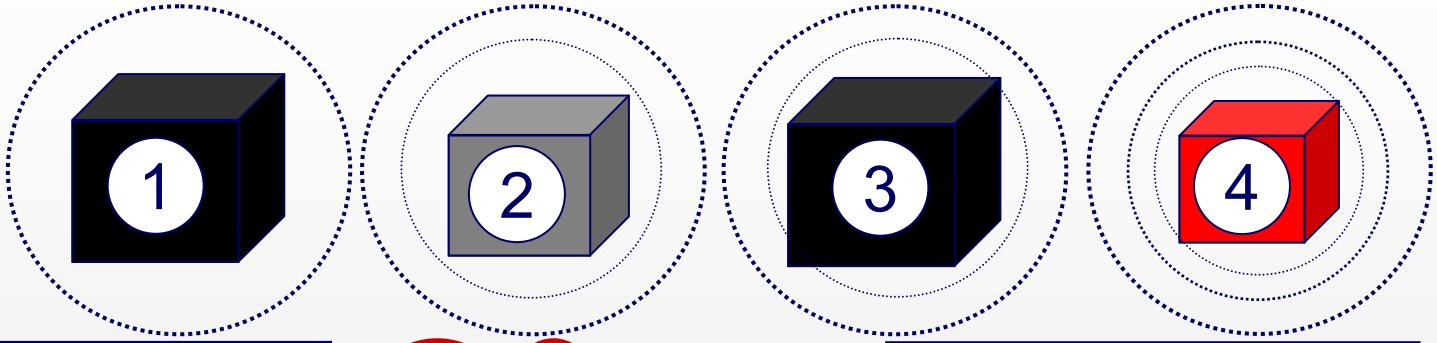
New

Choose 4

If switching costs are high, option 2 may be better choice (i.e. robust in value)

© 2007 Massachusetts Institute of Technology

Ex: Desiring "No" Change:
Value Robustness



Preferences t=1

Attribute	k_i
Size	0.5
Loudness	0.2

Choose 3

U(3)>U(2)>U(1)>U(4)

U(4)>U(2)>U(3)>U(1)

big>small

loud>quiet

red>gray>black

Change?

Preferences t=2

Attribute	k_i
Size	0.5
Loudness	0.2
Color	0.6

Attribute "priority"

New

Choose 4

If switching costs are high, option 2 may be better choice (i.e. robust in value)

Clever designs or *changeable designs* can achieve value robustness

© 2007 Massachusetts Institute of Technology

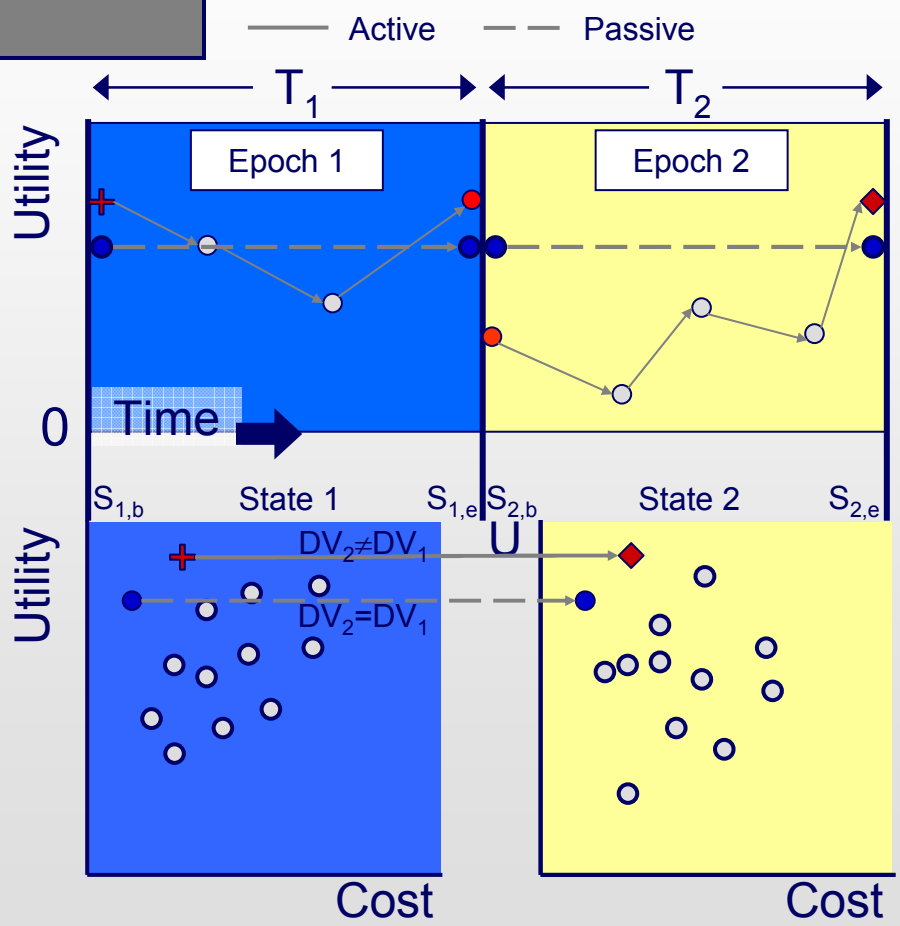
Achieving Value Robustness

Research suggests two strategies for "Value Robustness"

New Context Drivers

- External Constraints
- Design Technologies
- Value Expectations

1. Passive
   - Choose "clever" designs that remain high value
   - Quantifiable: Pareto Trace number
2. Active
   - Choose changeable designs that can deliver high value when needed
   - Quantifiable: Filtered Outdegree



Value robust designs can deliver value in spite of inevitable context change

© 2007 Massachusetts Institute of Technology

Designing for Value Robustness

Mindshift: recognize dynamic contexts and fallacy of static preferences; the inevitability of "change"

- Matching changing systems to changing needs leads to sustained system success
- Methods for increasing Changeability
  - Increase number of paths (change mechanisms)
  - Lower "cost" or increase acceptability threshold (apparent changeability)
- Concept-independent measure of changeability: filtered outdegree
  - Change mechanism drives filtered outdegree, as does consideration of alternative systems (future states)
  - Quantifiable filtered outdegree couples both objective and subjective measures (irreducible subjectivity → acceptability threshold)
- Changeability can be used as an explicit and consistent metric for designing systems

Designed for changeability, systems will be empowered to become value robust, delivering value in spite of context and preference changes

© 2007 Massachusetts Institute of Technology

SEAri Research Portfolio

DESIGNING for VALUE ROBUSTNESS

This area of research seeks to develop methods for concept exploration, architecting and design using a dynamic perspective for the purpose of realizing systems, products, and services that deliver sustained value to stakeholders in a changing world.

- Methods for dynamic multi-attribute trade space exploration
- Architecting principles and strategies for designing survivable systems
- Architecting strategies for coupling in system of systems
- Quantification of the changeability of a system design
- Techniques for the consideration of unarticulated and latent stakeholder value
- Taxonomy for enabling stakeholder dialogue on 'ilities'

Representations, analysis methods, and techniques for designing systems for "success" in dynamic contexts

© 2007 Massachusetts Institute of Technology

Access to Research

Navigation

Home

About

People

Research

Related Courses

Documents

Events

Sponsors

Community

Contact

Internal

Purpose

Web portal for sharing research within SEAri, MIT, and systems community

seari.mit.edu

© 2007 Massachusetts Institute of Technology

References

McManus, H.M., Richards, M.G., Ross, A.M., and Hastings, D.E., "A Framework for Incorporating "ilities" in Tradespace Studies," AIAA Space 2007, Long Beach, CA, September 2007.

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

Richards, M.G., Hastings, D.E., Rhodes, D.H., and Weigel, A.L., "Defining Survivability for Engineering Systems," 5th Conference on Systems Engineering Research, Hoboken, NJ, March 2007

Richards, M.G., *On-Orbit Serviceability of Space System Architectures*, Dual Master of Science Thesis, Aeronautics and Astronautics and Technology and Policy Program, MIT, June 2006

Ross, A.M., Rhodes, D.H., and Hastings, D.E., "Defining Changeability: Reconciling Flexibility, Adaptability, Scalability and Robustness for Maintaining Lifecycle Value," INCOSE International Symposium 2007, San Diego, CA, June 2007.

Ross, A.M. and Rhodes, D.H., "The System Shell as a Construct for Mitigating the Impact of Changing Contexts by Creating Opportunities for Value Robustness," 1st Annual IEEE Systems Conference, Honolulu, HI, April 2007.

Ross, A.M. and Hastings, D.E., "Assessing Changeability in Aerospace Systems Architecting and Design Using Dynamic Multi-Attribute Tradespace Exploration," AIAA Space 2006, San Jose, CA, September 2006.

Ross, A.M. *Managing Unarticulated Value: Changeability in Multi-Attribute Tradespace Exploration*, Doctor of Philosophy Dissertation, Engineering Systems Division, MIT, June 2006

Ross, A.M. *Multi-Attribute Tradespace Exploration with Concurrent Design as a Value-centric Framework for Space System Architecture and Design*, Dual Master of Science Thesis, Aeronautics and Astronautics and Technology and Policy Program, MIT, June 2003

© 2007 Massachusetts Institute of Technology

QUESTIONS

http://seari.mit.edu

rhodes@mit.edu

adamross@mit.edu