System Architecting for Survivability:

Limitations of Existing Methods for Aerospace Systems

2008 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

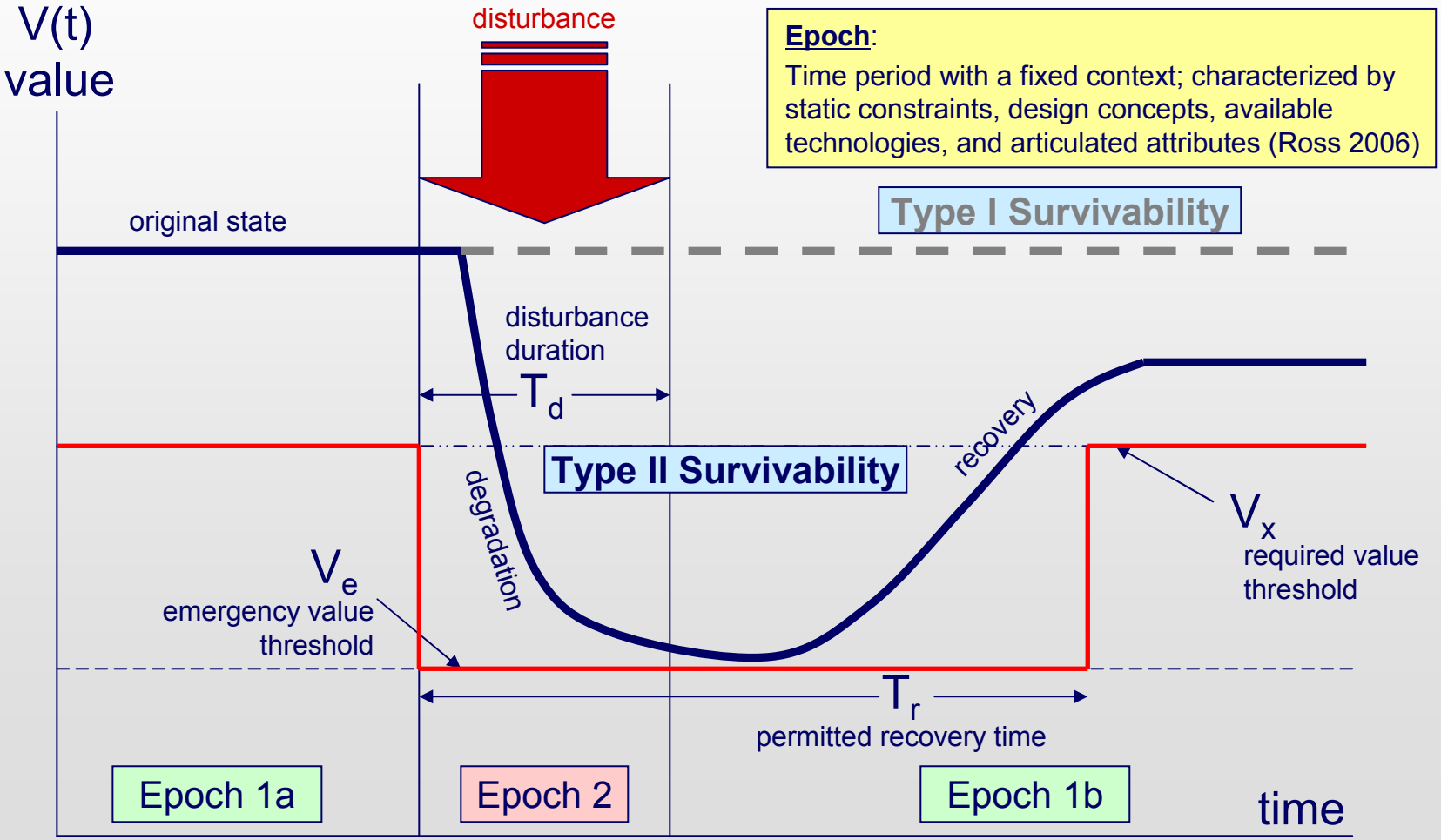
Agenda

- Survivability Definition
- Literature Review
  - Research Context
  - Motivation: Space System Fragility
  - Limitations of Survivability Methods
- Future Work
- Conclusion

© 2008 Massachusetts Institute of Technology

Definition of Survivability

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



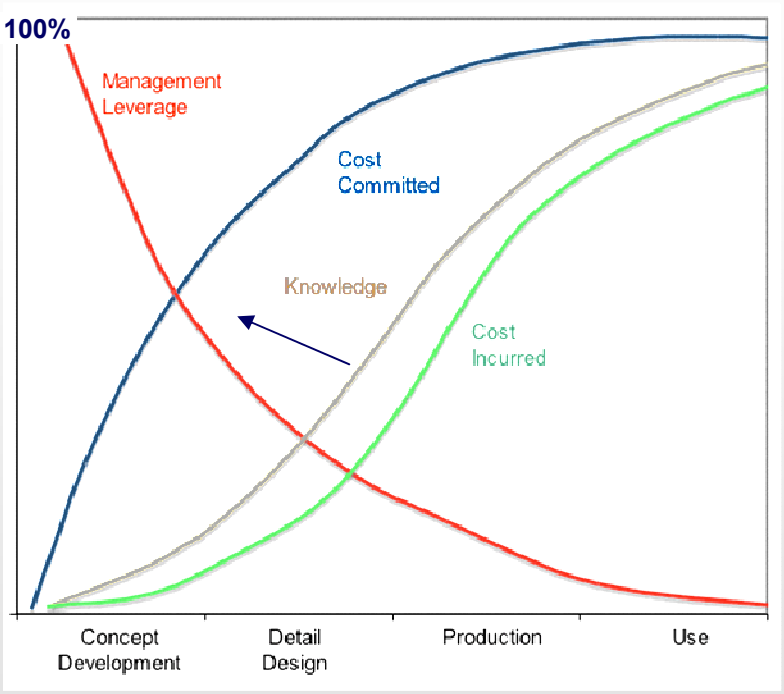
Epoch:
Time period with a fixed context; characterized by static constraints, design concepts, available technologies, and articulated attributes (Ross 2006)

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

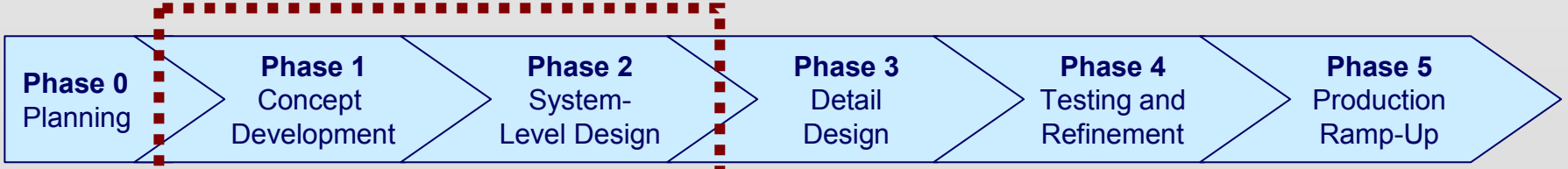
System Architecture in Product Design and Development

- Ulrich and Eppinger (2004) have six-phase model of product development
- Research addresses product architecture; spanning Phases 1 and 2
  - Concept Development
    - Identification of stakeholders
    - Enumeration and evaluation of design alternatives
    - Selection of one or more concepts for further development
  - System-Level Design
    - Definition of the architecture, including subsystem decompositions and functional specifications

Critical front-end in complex system design



(Gruhl 1992; Blanchard and Fabrycky 2006)



(Ulrich and Eppinger 2004)

© 2008 Massachusetts Institute of Technology

Value-Based Conceptual Design Through Tradespace Exploration

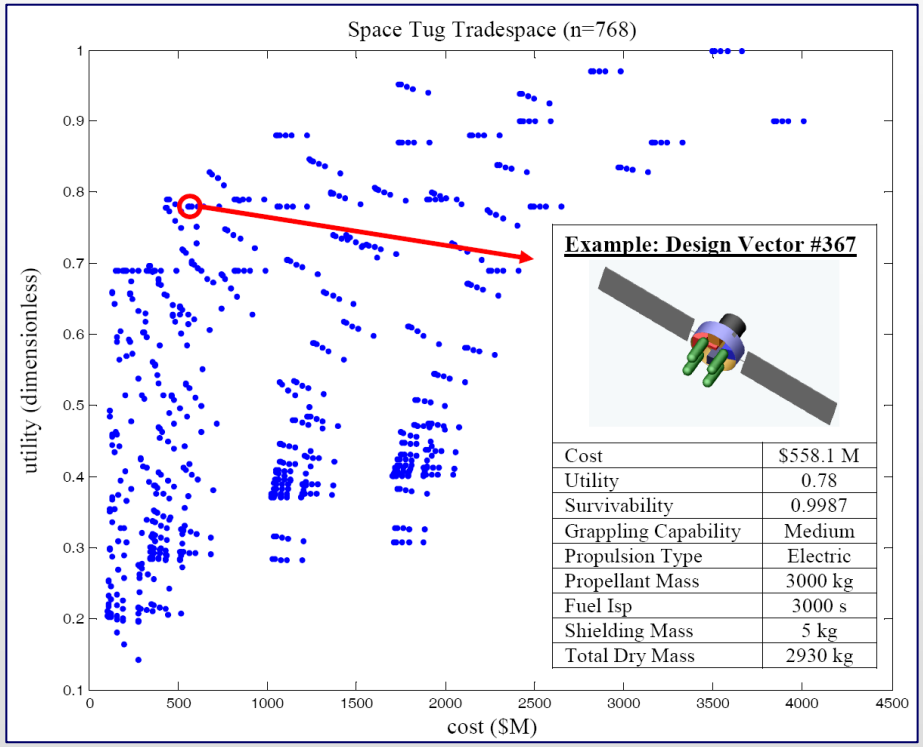
Value is a measure of net benefit specified by a stakeholder

- Value-centric perspective enables unified evaluation of technically diverse system concepts
- Operationalized through the application of decision theory to engineering design
  - Quantifies benefits, costs, and risks

    (Thurston 1990; Keeney and Raiffa 1993)

- Tradespace exploration uses computer-based models to compare thousands of architectures
  - Avoids limits of local point solutions
  - Maps decision maker preference structure to potential designs

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



© 2008 Massachusetts Institute of Technology

Incorporating Survivability into Tradespace Studies

*Ilities are temporal system properties that specify the degree to which systems are able to maintain or even improve value in the presence of change**

- Ilities are increasingly regarded as ***critical system properties*** for delivering stakeholder value

  (Moses 2004; Rhodes 2004; McManus and Hastings 2006)

- ***Ongoing research*** seeks to establish prescriptive methods for incorporating ilities in system design

  (de Neufville 2004; de Weck, de Neufville and Chaize 2004; Fricke and Schulz 2005; Rajan, Van Wie et al. 2005; Ross and Hastings 2006; Nilchiani and Hastings 2007; Silver and de Weck 2007)

- ***Challenges*** for incorporating ilities in tradespace studies
  - Taxonomic uniformity
  - Characterizing temporal constructs in traditional tradespaces
  - Disaggregating from traditional attributes in Multi-Attribute Utility Theory
  - Investing in uncertain future

*Definition excludes some non-operational ilities, such as manufacturability

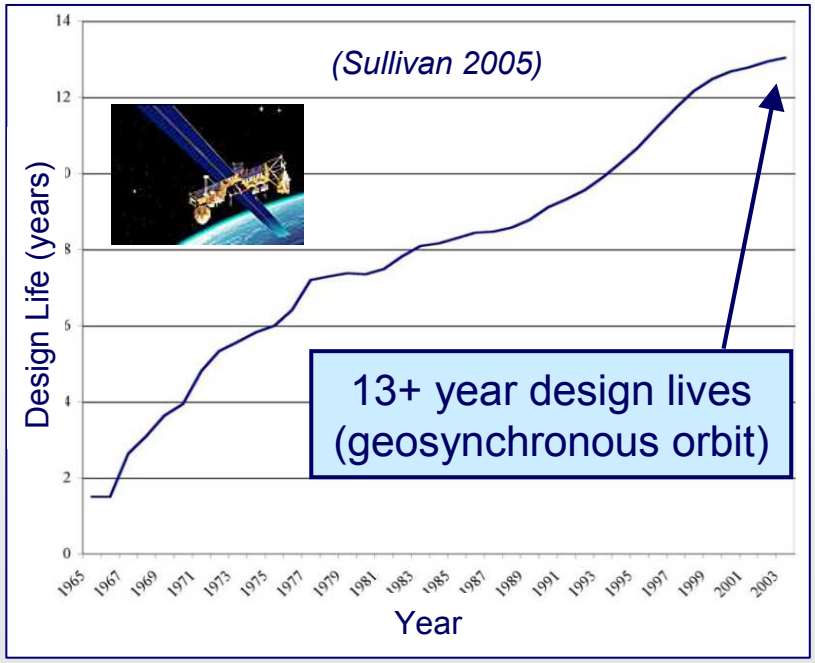
*McManus, H., Richards, M., Ross, A., and Hastings, D., "A Framework for Incorporating "ilities" in Tradespace Studies," *AIAA Space 2007*, Long Beach, CA, September 2007.

Motivation: Need for "ilities" in Space Architecture

1960's Paradigm

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

Evolution to Current State

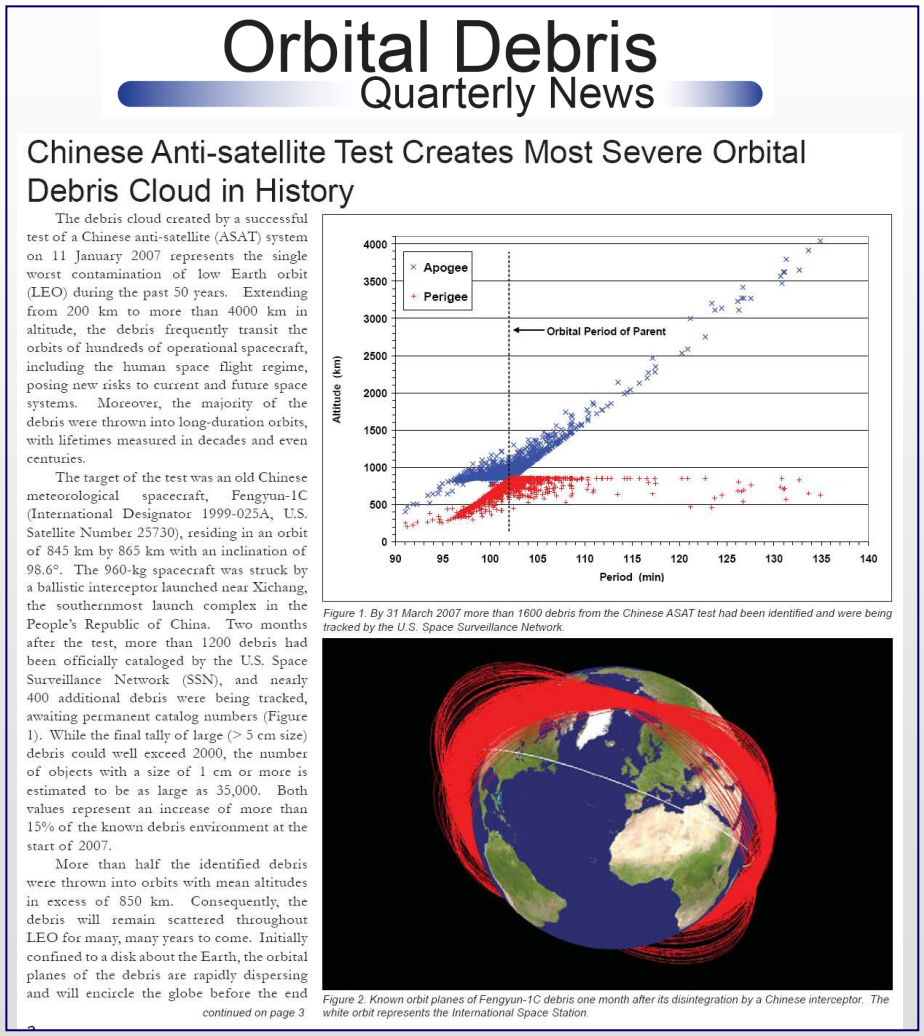


- **Inability to adapt to uncertain future environments, including disturbances**

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

© 2008 Massachusetts Institute of Technology

Criticality of Survivability for U.S. Space Architectures



Orbital Debris
Quarterly News

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

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

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

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

continued on page 3

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

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

1. Growth of military and commercial dependency on space systems

   (Gonzales 1999; GAO 2002; Ballhaus 2005)

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

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

3. Proliferation of threats

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

4. Weakening of the sanctuary view in military space policy

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

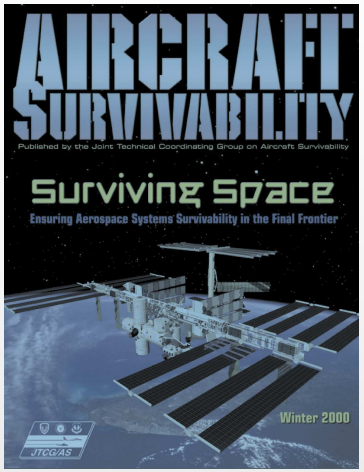
© 2008 Massachusetts Institute of Technology

Current Response: Survivability Engineering

- Survivability engineering discipline emerged in 1960's
  - Survivability requirements derived early in conceptual design from System Threat Assessment Report (STAR)
  - Survivability evaluated using Probabilistic Risk Assessment

    (Ball 2003; USAF 2005)
- Survivability of individual systems well addressed

  (Nordin and Kong 1999, Paterson 1999)



- However, architecting for survivability is poorly understood
  - e.g., survivability of triad of U.S. strategic forces

    (Bracken 1983; Blair 1985)
  - Criticality of whole product system

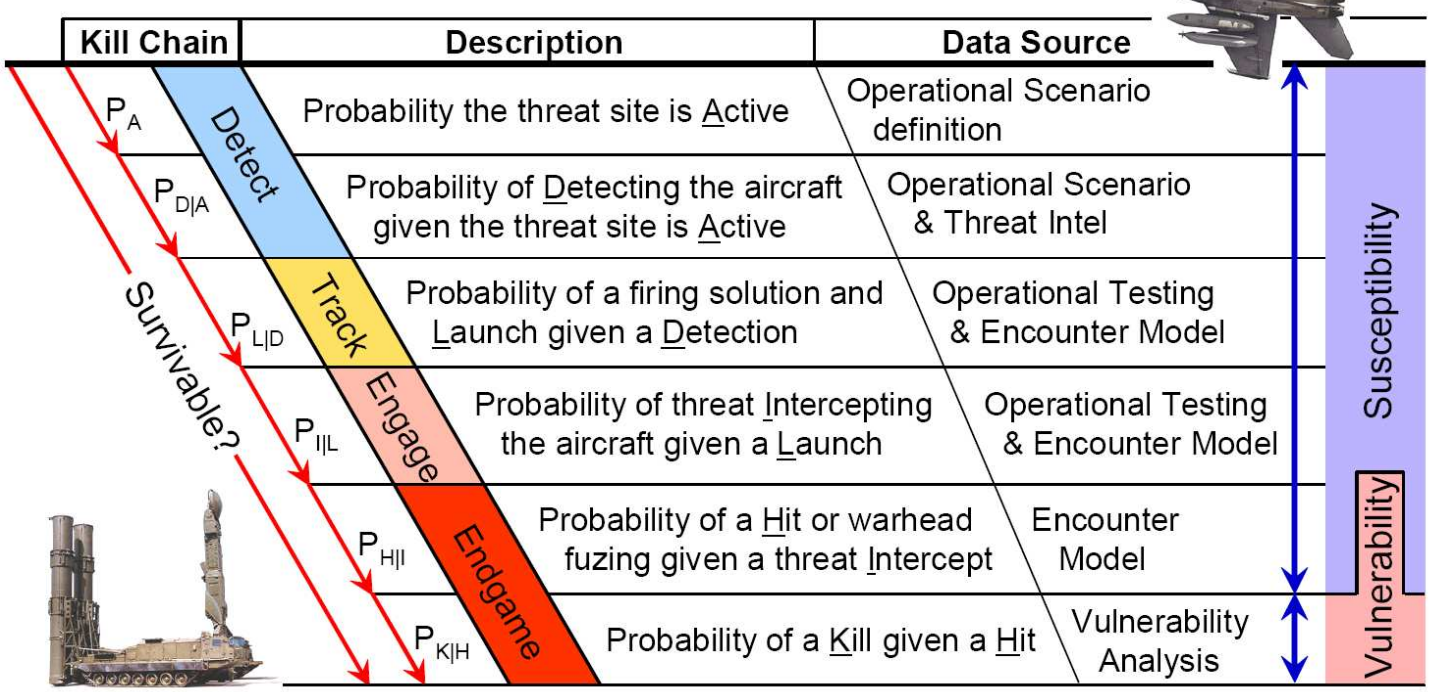
    (Leveson 2002; Sheffi 2005; Baldwin et al. 2006; Hollnagel, Woods and Leveson 2006)

How to evaluate survivability as an emergent architectural property?

© 2008 Massachusetts Institute of Technology

Kill Chain for Engagement-Level Survivability Assessment

$$P_S = 1 - P_K = 1 - P_H \cdot P_{K/H}$$



Anderson, T. and J. Williamsen (2007). "Force Protection Evaluation for Combat Aircraft Crews." *48th AIAA Structures, Structural Dynamics, and Materials Conference*, Honolulu, HI.

© 2008 Massachusetts Institute of Technology

Problems with Existing Metrics

Engagement Survivability	$P_S = 1 - P_K = 1 - P_H \cdot P_{K/H}$ S = survive, K = kill, H = hit	• Binary assessment criteria fails to internalize graceful degradation
Campaign Survivability	$CS = (P_S)^N = (1 - P_K)^N$ N = number of engagements	• Binary assessment criteria • Assumes independence among shot and mission outcomes
Reliability Function (aka Survival Function)	$R(t) = 1 - F(t) = e^{t/MTBF}$ t = operating time MTBF = mean time between failure	• Construct validity • Binary assessment criteria • Time to failure assumed as exponential density function
Inherent Availability	$A_i = \frac{MTBF}{MTBF + MTTR}$ MTTR = mean time to repair	• Construct validity • Binary assessment criteria

(Ball 2003; Blanchard and Fabrycky 2006)

© 2008 Massachusetts Institute of Technology

Limitations of Survivability Engineering

1. Treatment of survivability as a **constraint** rather than an active trade in the design process

   (Wheelon 1997; Walker 2007)

2. **Static** nature of System Threat Assessment Reports

   (Ball 2003; Anderson and Williamsen 2007)

3. Reliance on probabilistic risk assessment and the assumption of **independent** failures

   (Leveson 1995; Perrow 1999; Leveson 2002; Pate-Cornell, Dillon and Guikema 2004)

4. Limited **scope** of survivability design and analysis

   (Neumann 2000; USAF 2005; Walker 2007)

5. Lack of **value-centric** perspective

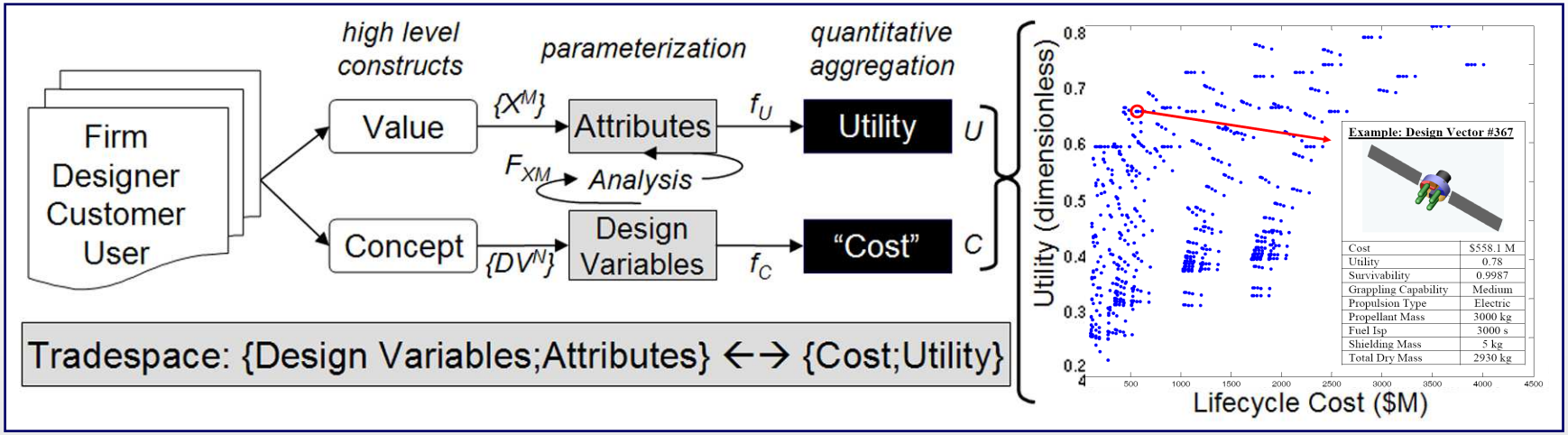
   (Keeney 1992; Ross 2006)

© 2008 Massachusetts Institute of Technology

Future Work: Dynamic Modeling of Survivability

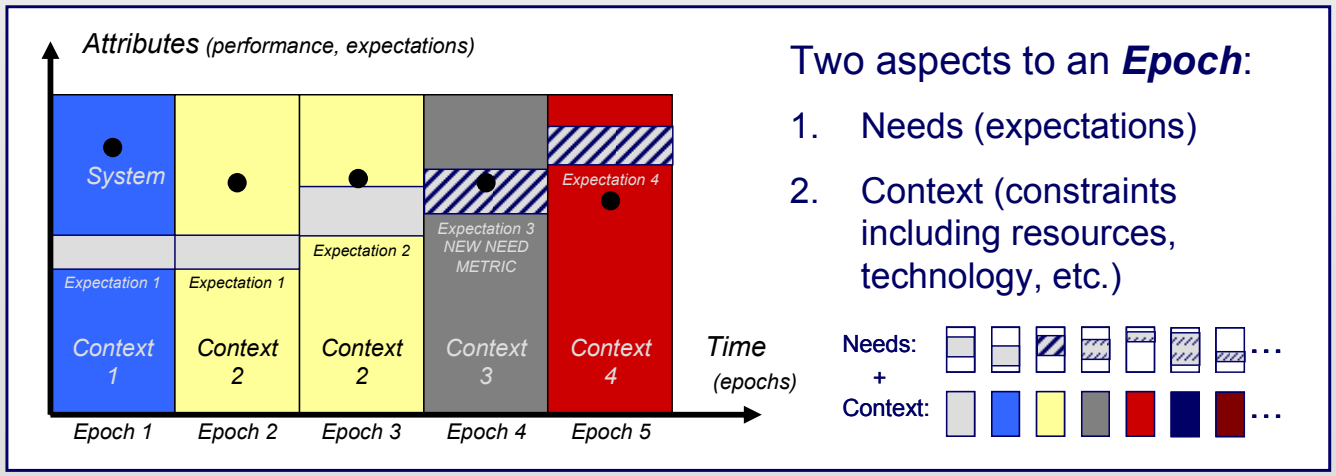
Multi-Attribute Tradespace Exploration (MATE)

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



Epoch-Era Analysis

(Ross 2006)



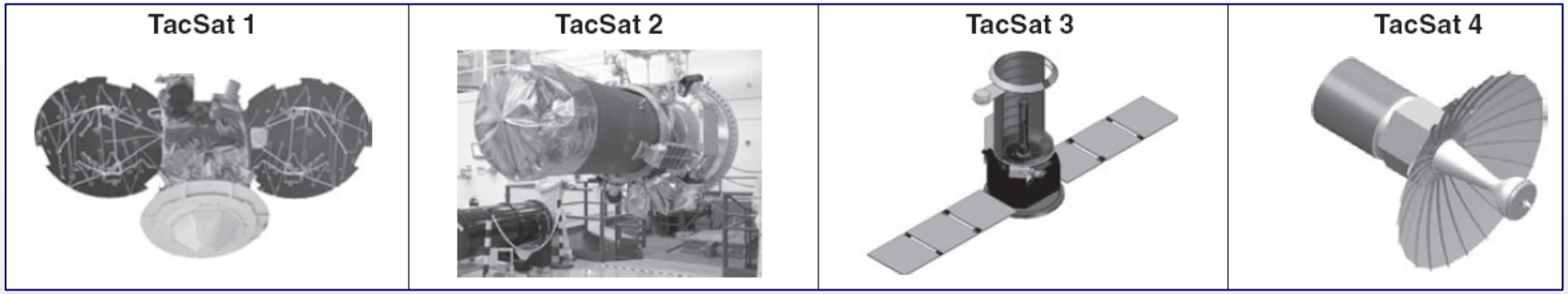
Two aspects to an ***Epoch***:

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

© 2008 Massachusetts Institute of Technology

Future Case Application: Operationally Responsive Space

Operationally Responsive Space (ORS) ***purportedly enhances survivability*** of current national space architecture



(GAO 2006)

- Goal: reduce time constants associated with space system acquisition, design, and operation *(DoD 2007)*
- Fundamental idea: trade off reliability and performance of "big space" for speed, responsiveness, and customization potentially offered by small tactical spacecraft (TACSATs)
- Problem: uncertain value proposition *(Tomme 2006; Fram 2007)*

"ORS deserves, yet has not received, our analytic due diligence."
(Mr. Gil Klinger, Former Director of Space Policy, U.S. National Security Council, 22 August 2007)

© 2008 Massachusetts Institute of Technology

Conclusion

- Given limitations of survivability engineering for aerospace systems, need design methodology that:

1. incorporates survivability as an **active trade** throughout design process
2. reflects **dynamics** of operational environments over entire lifecycle
3. captures **path dependencies** of system susceptibility and vulnerability
4. extends in scope to **architecture-level** survivability assessments
5. takes a **value-centric** perspective

- Opportunity to build on recent research on dynamic tradespace exploration
- Application of emergent survivability design method may aid in resolution of critical issue in national space architecture
  - Existing analytic frameworks not well-suited to evaluating purported survivability benefits of Operationally Responsive Space (ORS)*

* Small spacecraft paradigm emphasizing timely launch, tactical control, and customization

© 2008 Massachusetts Institute of Technology

Thank You / Questions?

References (1/4)

- Anderson, T. and J. Williamsen (2007). "Force Protection Evaluation for Combat Aircraft Crews." *48th AIAA Structures, Structural Dynamics, and Materials Conference*, Honolulu, HI.
- Baldwin, C., M. Komaroff and P. Croll (2006). "Systems Assurance - Delivering Mission Success in the Face of Developing Threats." *A White Paper from NDIA Systems Assurance Committee*.
- Ball, R. (2003). The Fundamentals of Aircraft Combat Survivability Analysis and Design. Reston, American Institute of Aeronautics and Astronautics.
- Blair, B. (1985). Strategic Command and Control: Redefining the Nuclear Threat. Washington D.C., Brooking Institution Press.
- Blanchard, B. and W. Fabrycky (2006). Systems Engineering and Analysis. Upper Saddle River, Prentice Hall.
- Bracken, P. (1983). The Command and Control of Nuclear Forces. New Haven, Yale University Press.
- de Neufville, R. (2004). "Uncertainty Management for Engineering Systems Planning and Design." *MIT Engineering Systems Symposium*, Cambridge, MA.
- de Weck, O., R. de Neufville and M. Chaize (2004). "Staged Deployment of Communications Satellite Constellations in Low Earth Orbit." *Journal of Aerospace Computing, Information, and Communication,* 1(3): 119-136.
- DoD (2003). "Department of Defense Architecture Framework: Version 1.0." *DoD Architecture Framework Working Group.*
- DoD (2007). "Plan for Operationally Responsive Space: A Report to Congressional Defense Committees." *National Security Space Office*. Washington, DC.

© 2008 Massachusetts Institute of Technology

References (2/4)

- Fricke, E. and A. Schulz (2005). "Design for Changeability (DfC): Principles to Enable Changes in Systems Throughout Their Entire Lifecycle." *Systems Engineering,* 8(4): 342-359.
- Gruhl, W. (1992). "Lessons Learned, Cost/Schedule Assessment Guide." *Internal presentation*, NASA Comptroller's Office.
- Hollnagel, E., D. Woods and N. Leveson (2006). Resilience Engineering: Concepts and Precepts. Hampshire, UK, Ashgate.
- Keeney, R. (1992). Value-Focused Thinking: A Path to Creative Decisionmaking. Cambridge, Harvard University Press.
- Keeney, R. and H. Raiffa (1993). Decisions with Multiple Objectives: Preferences and Value Tradeoffs. Cambridge, Cambridge University Press.
- Leveson, N. (1995). Safeware: System Safety and Computers. Boston, Addison-Wesley.
- Leveson, N. (2002). System Safety Engineering: Back to the Future. Cambridge, MIT Department of Aeronautics and Astronautics.
- Maier, M. and E. Rechtin (2002). The Art of Systems Architecting. Boca Raton, CRC Press.
- McManus, H. and D. Hastings (2006). "A Framework for Understanding Uncertainty and its Mitigation and Exploitation in Complex Systems." *IEEE Engineering Management Review,* 34(3): 81-94.
- McManus, H., D. Hastings and J. Warmkessel (2004). "New Methods for Rapid Architecture Selection and Conceptual Design." *Journal of Spacecraft and Rockets,* 41(1): 10-19.

© 2008 Massachusetts Institute of Technology

References (3/4)

- Moses, J. (2004). "Foundational Issues in Engineering Systems: A Framing Paper." *MIT Engineering Systems Symposium*, Cambridge, MA.
- Neumann, P. (2000). "Practical Architectures for Survivable Systems and Networks." *Prepared by SRI International for the U.S. Army Research Laboratory*.
- Nilchiani, R. and D. Hastings (2007). "Measuring the Value of Flexibility in Space Systems: A Six-Element Framework." *Systems Engineering,* 10(1): 26-44.
- Nordin, P. and M. Kong (1999). Chapter 8.2 Hardness and Survivability Requirements. Space Mission Analysis and Design. El Segundo, Microcosm Press.
- Pate-Cornell, M., R. Dillon and S. Guikema (2004). "On the Limitations of Redundancies in the Improvement of System Reliability." *Risk Analysis,* 24(6): 1423-1436.
- Paterson, J. (1999). "Overview of Low Observable Technology and Its Effects on Combat Aircraft Survivability." *Journal of Aircraft*, 36(2): 380-388.
- Perrow, C. (1999). Normal Accidents: Living with High-Risk Technologies. Princeton, Princeton University Press.
- Rajan, P., M. Van Wie, M. Campbell, K. Wood and K. Otto (2005). "An Empirical Foundation for Product Flexibility." *Design Studies,* 26(4): 405-438.
- Rhodes, D. (2004). "Report on Air Force/LAI Workshop on Systems Engineering for Robustness." Arlington, VA.
- Ross, A., D. Hastings, J. Warmkessel and N. Diller (2004). "Multi-Attribute Tradespace Exploration as Front End for Effective Space System Design." *Journal of Spacecraft and Rockets,* 41(1): 20-28.

© 2008 Massachusetts Institute of Technology

References (4/4)

- Ross, A. (2006). "Managing Unarticulated Value: Changeability in Multi-Attribute Tradespace Exploration." Doctoral dissertation, Engineering Systems Division, Massachusetts Institute of Technology, Cambridge, MA.
- Ross, A. and D. Hastings (2006). "Assessing Changeability in Aerospace Systems Architecting and Design Using Dynamic Multi-Attribute Tradespace Exploration." *AIAA Space 2006*, San Jose, CA.
- Sheffi, Y. (2005). The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage. Cambridge, The MIT Press.
- Sullivan, B. (2005). "Technical and Economic Feasibility of Telerobotic On-Orbit Satellite Servicing." Doctoral dissertation, Department of Aerospace Engineering, University of Maryland, College Park, MD.
- Ulrich, K. and S. Eppinger (2004). Product Design and Development. Boston, McGraw Hill.
- USAF (2005). "SMC Systems Engineering Primer and Handbook." *Space & Missile Systems Center, U.S. Air Force*.
- Walker, D. (2007). Personal conversation with Donald Walker, Senior Vice President of Systems Planning and Engineering, Aerospace Corporation, 12 January 2007.
- Walton, M. and D. Hastings (2004). "Applications of Uncertainty Analysis to Architecture Selection of Satellite Systems." *Journal of Spacecraft and Rockets*, 41(1): 75-84.
- Weigel, A. and D. Hastings (2004). "Measuring the Value of Designing for Future Downward Budget Instabilities." *Journal of Spacecraft and Rockets*, 41(1): 111-119.
- Wheelon, A. (1997). "CORONA: The First Reconnaissance Satellites." *Physics Today*, February 1997, pp. 24-30.

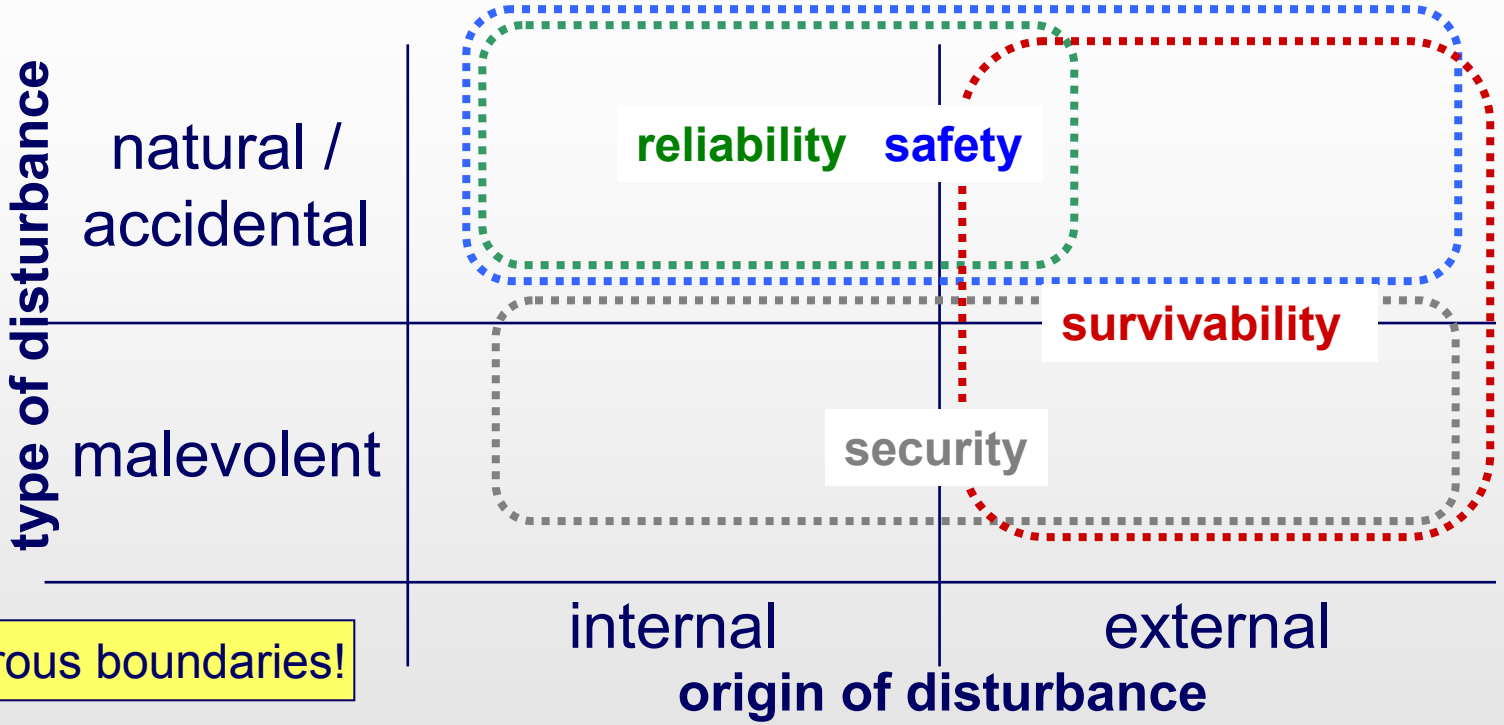
© 2008 Massachusetts Institute of Technology

Terminology

- Architecture
  - the structure of components, their relationships, and the principles governing their design and evolution over time (DoD 2003)
- Architecting
  - the process of creating and building architectures; those aspects of a system development most concerned with conceptualization, objective definition, and certification for use (Maier and Rechtin 2002)
- Design
  - [V] the process of devising a system, component or process to meet desired needs….[includes] the establishment of objectives and criteria, synthesis, analysis, construction, testing, and evaluation (Accreditation Board for Engineering and Technology)
  - [N] the detailed formulation of the plans or instructions for making a defined system element (Maier and Rechtin 2002)
- Tradespace
  - the potential solution space spanned by completely enumerated design variables; enables cross-design comparisons (Ross and Hastings et al. 2004)

© 2008 Massachusetts Institute of Technology

Survivability Mapping to Related Disciplines



reliability	probability of functioning for a prescribed time under stipulated environmental conditions
safety	freedom from accidents or losses
security	protection of a system's informational, operational, and physical elements from malicious intent
survivability	capability to avoid or withstand hostile natural and synthetic environments

(Leveson 1995; USAF 2005)

© 2008 Massachusetts Institute of Technology

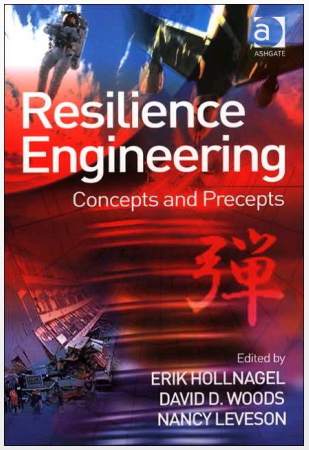
Resilience Engineering

Brittleness ← **reliability engineering** — **system safety engineering** → **Resilience**

Research Agenda for Systems of Systems (SoS) Architecting

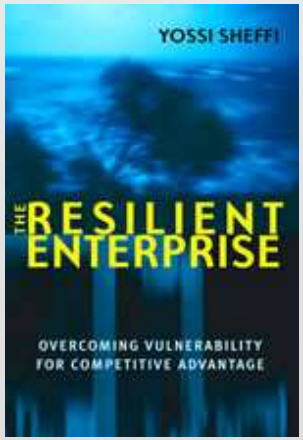
1. Resilience
2. Illustration of Success
3. System vs. SoS Attributes
4. Model Driven Architecting
5. Multiple SoS Architectural Views
6. Human Limits to Handling Complexity
7. Net-Centric Vulnerability
8. Evolution
9. Guided Emergence
10. No Single Owner SoS

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



© 2008 Massachusetts Institute of Technology