2011 SEAri Annual Research Summit

Research Report

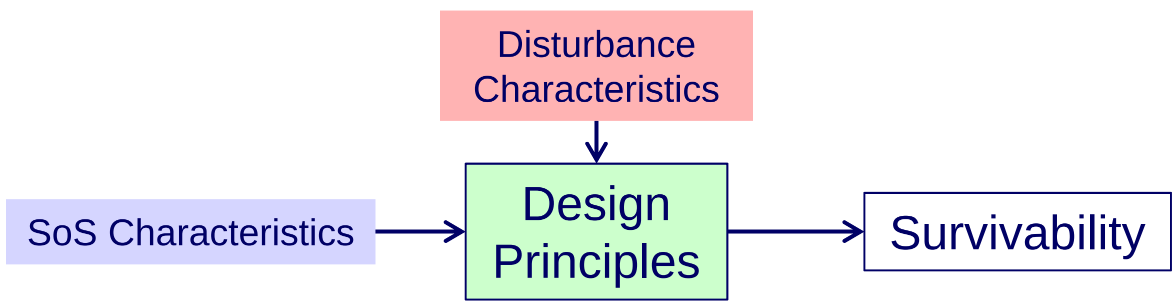
"Examining Survivability of Systems of Systems"

Brian Mekdeci, ESD PhD Candidate

October 21, 2011
Cambridge, MA
Massachusetts Institute of Technology

Topics

- Motivations and prior survivability research
- Characterizing disturbances
- Distinguishing SoS from traditional systems – implications for survivability
- Research directions



Talk presents preliminary examination of how some characteristic properties of SoS may enable or hinder survivability based on existing design principles and proposed taxonomy of disturbances

Motivations and Prior Research

System Complexity as a Driving Factor for Survivability Research

Failures of large, complex systems have been prominent in recent news:

- Japanese nuclear power plants
- Sony PlayStation Network (PSN)
- Amazon Cloud Service

Stakeholders want systems with acceptable value

- Over long life cycle
- Requires balancing performance, cost, risk
- Subject to various disturbances / context changes

http://kbmt.images.worldnow.com

Particularly problematic in systems of systems (SoS) with diverse stakeholders (Ellison & Woody 2007) **due to variation in**:

- Information about the system
- Needs & expectations
- Risk management strategies
- Resources

http://nytimes.com

As traditional systems get interconnected and overall complexity increases designers, architects and decision makers need design principles that will enable and enhance system and SoS survivability

Survivability Research Questions (2006-2009)

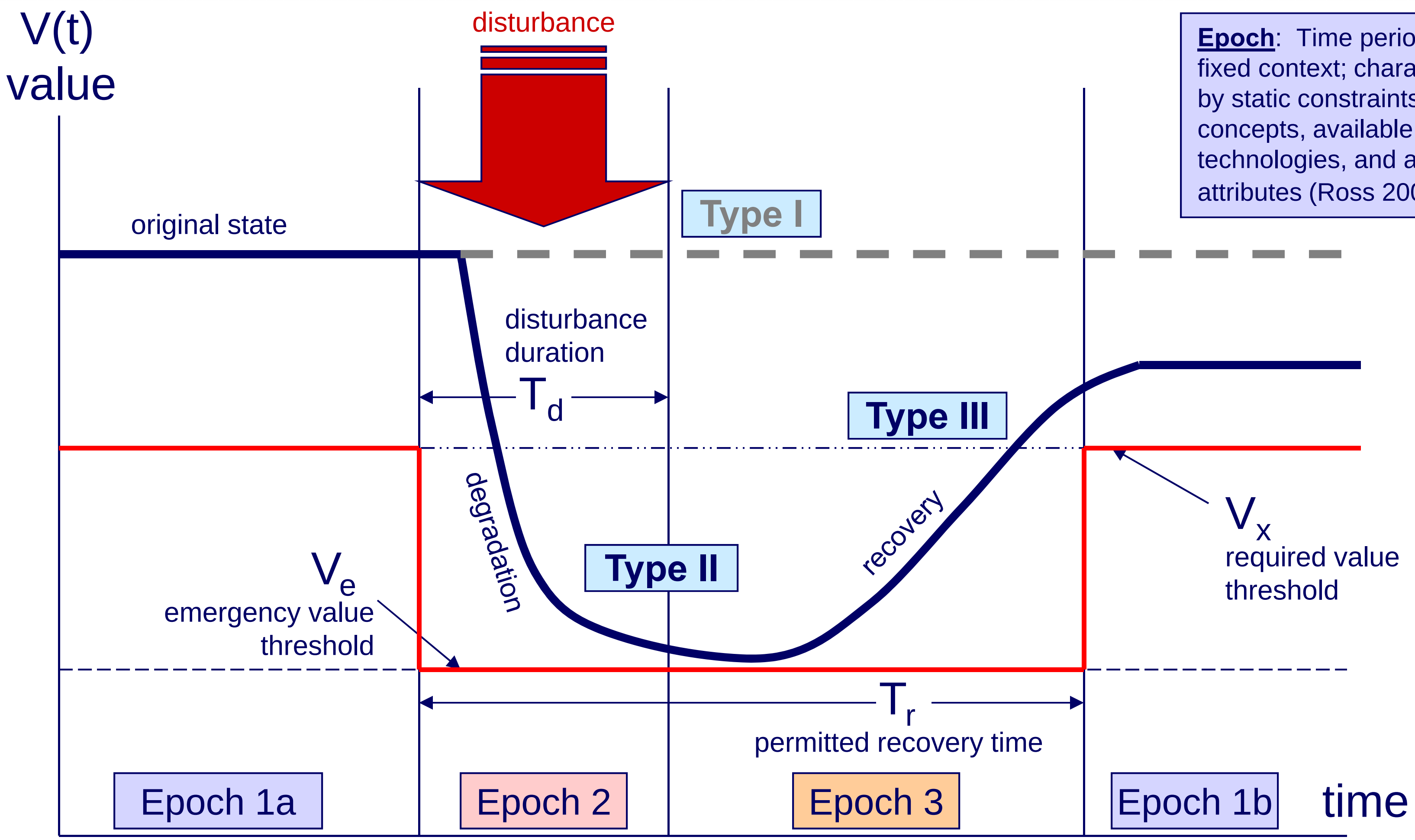
1. What is a dynamic, operational, and value-centric **definition** of survivability for engineering systems?
   - ✓ **Value based definition with three types of survivability**
2. What **design principles** enable survivability?
   - ✓ **17 design principles for system survivability derived**
3. How can survivability be quantified and used as a **decision metric in exploring tradespaces** during conceptual design of aerospace systems?
   - ✓ **Two new metrics developed**
4. For a given mission, how to **evaluate the survivability of alternative system architectures** in dynamic disturbance environments?
   - ✓ **MIT SEAri's Multi-Attribute Tradespace Exploration (MATE) method extended for survivability trade-offs**

Research built on a decade of foundational research on value-driven methods for tradespace exploration

Definition of Survivability

(Richards, 2009)

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)

Survivability Design Principles

(Richards, 2009)

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

Methodological Insights
Prior Survivability Research

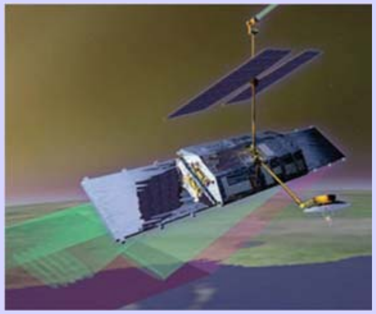
Multi-Attribute Tradespace Exploration adapted for Survivability ***incorporates survivability as a decision metric*** into conceptual design

- Design principles reveal latent survivability trades and inform selection of survivability design variables
- Survivability metrics enable discrimination among thousands of concept design alternatives

MATE for Survivability ***improves on existing tradespace approaches***

- Pareto front in traditional tradespace exploration studies excludes most survivable designs
- Evaluates survivability implications for selection of baseline architecture

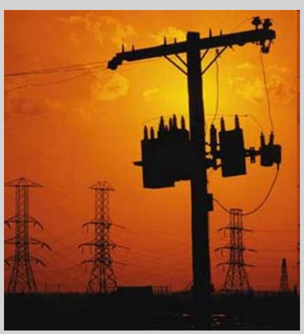
CASE APPLICATION



*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.*

2009 Research Recommendations for Further Research

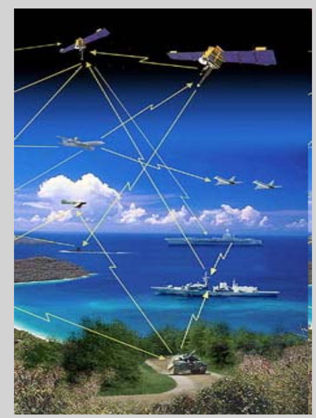
- **Extend scope to systems-of-systems (SoS)**
- Incorporate Concept of Operation (CONOPs)
  - *CONOPs may be more important consideration for SoS due to potential lack of control over constituent design*
- Apply Tradespace Exploration method (MATE) for Survivability to additional system cases for prescriptive insights



power distribution

transportation

water distribution



communications

Richards, 2009

Current SoS Survivability Research (2010-2012)

Characterizing Disturbances

Characterizing Disturbances

Nature

- Is disturbance natural or artificial
- How does the disturbance impact the system?

Origin

- Internal or external to the system
  - For many SoS, the lines are blurred.

Intent

- Is there an intent, by some entity, to cause this disturbance?
- Is the intent benign or malicious?

Duration of Impact

- How long is the duration of the disturbance?
- Does the original context resume?

Effectiveness of a survivability design principle will be strongly dependent on characteristics of the disturbances and the system

Using Passive Capabilities to Reduce Susceptibility to Natural Disturbances

Are the 17 Survivability Design Principles Enough?

What about susceptibility to natural disturbances?

- Robots aren't susceptible to disease
- Humans aren't susceptible to rust

Lightning rods & protectors

- Passive devices, attached to buildings, airplanes *actually draw lightning to the object!*
  - to safely dissipate it
- Reduces susceptibility to fires, electrocutions
- Poorly designed entities can act like a lightning rod and be damaged!

http://www.pbase.com/aestus/image/78856538

New Design Principle: Redirect disturbances away from vulnerable components

Complex Origins of Disturbances

Sun evaporates lakes → Evaporated water forms clouds → rainfall →decreased visibility →loss of situational awareness →failure to maintain minimum separation →crash →loss of life, system

- Decreased visibility also impacts ability to identify and detect targets.
- Decreased visibility can also be caused by a different CONOPS, such as flying the UAV at night instead of the day
- Corrosion leads to component failure, which can have multiple impacts, including reduced ability to identify and detect targets
- Corrosion can also be caused by a different CONOPs such as flying the vehicle at low altitude, over a large body of salt water

Complex Causes and Impact

<u>2003 North American Blackout</u>

- 2nd largest blackout in the world (ever)
  - 55 million affected
- What caused it?
  - Overgrown trees tripped power lines
  - Ohio power station had bug in monitoring software, did not handle load switching properly
  - Load moved to other lines, which became overloaded, increasing load on nearby lines, etc.
  - Cascading failure caused by a chain of disturbances

Due to complexity of systems of systems, disturbances may not be simple, single-event occurrences

- May have multiple causes
- May have multiple impacts

2011 SEAri Research Summit

Complex Disturbances: Sony PlayStation Network Outage

Sony PlayStation Network (PSN)

- Allows users to play games, download movies & music, social network
- Approximately 130 servers, 50 software programs and 77 million users

Cyber Attack and PSN Outage

- Sony took entire system down on April 20, 2011 after an “external intrusion”
  - Breach occurred after “a month and a half” of attacks (Joystiq, 2011)
  - Sony took 23 days to put the system back online
    - Initially said that it would take “a day or two”

Personal data from 77 million users stolen

- One of the largest data breaches in history (CBC News, 2011)
- Users were not notified of stolen data until May 2, 2011
- Data was unencrypted

Required both “fixing” and “enhancing” the network

Complex Disturbances: Sony PlayStation Network Outage

Sony PlayStation Network (PSN)

- Allows users to play games, download movies & music, social network
- Approximately 130 servers, 50 software programs and 77 million users

Cyber Attack and PSN Outage

- Sony took entire system down on April 20, 2011 after an "external intrusion"
  - Breach occurred after "a month and a half" of attacks (Joystiq, 2011)
  - Sony took 23 days to put the system back online

Repercussions

$171 million in costs (so far)
Class action lawsuit
Government investigations (possible fines)
User backlash

PLAYSTATION® Network

Sony stated that providing details of the attack "could be used to exploit vulnerabilities in systems other than Sony's that have similar architecture to the PSN" (Sony letter to US Congress, 2011)

Properties Distinguishing SoS from Traditional System

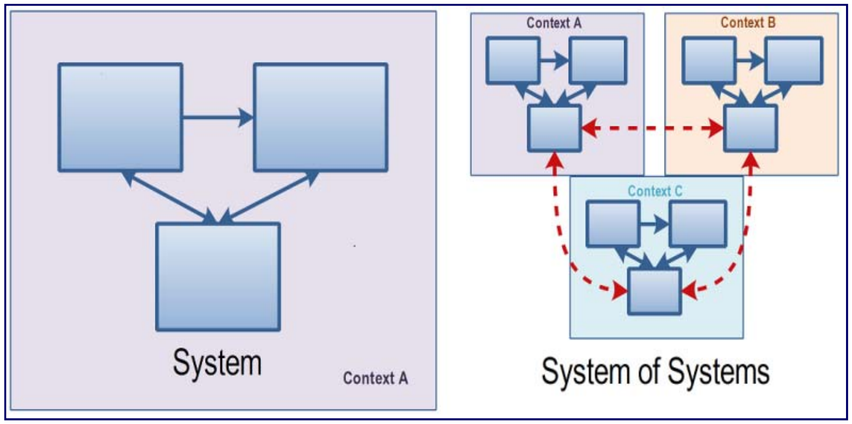
Implications for Survivability

Whether a particular SoS characteristic is going to enable or hinder survivability, will depend on disturbance and context in which system operates

Increased Contextual Diversity
(Shah 2007)

Components (constituent systems) in SoS more likely to be physically separated than components in traditional systems, so more likely to be operating under different environmental conditions

With managerial independence, components in SoS more likely to be operated with different stakeholder needs/expectations



Survivability Impact: Multiple system contexts increase the probability of disturbances in overall SoS

Geographic Separation
(Maier 1998)

- Directly enables design principles of *concealment, distribution, containment*
- Components may have different environmental contexts, increasing probability of disturbance
- Separation of components creates local knowledge that must be shared, reducing ease of coordination of components

<ins>Survivability Impact</ins>: Geographic separation may both enable or hinder survivability

Component Independence
(Maier 1998)

- SoS often have managerial and/or operational independence of the components
- Enables survivability in that local decisions or operational changes can be used to respond/prevent local disturbances
- Could reduce SoS survivability in that local decisions or controls may not always be in the interests of global level survivability

Survivability Impact: Component independence may enable component survivability, but may make SoS level survivability more difficult

Evolutionary Development
(Maier 1998)

- Traditional systems typically designed and assembled prior to operations
- SoS components often added or removed dynamically, during operation of SoS – constantly evolving
- Enables survivability in that there may be intermediate forms that SoS can “fall back to”
- Lessens survivability in that multiple vendors, protocols, product generations make reliability difficult to achieve
- Threat to survivability if SoS evolves toward an unmanageable state

Survivability Impact: Evolutionary development may both enable or hinder survivability

Decreased System Awareness

Since SoS constituents often operating/controlled somewhat independently under differing contexts, must share contextual information on timely basis, depending upon:

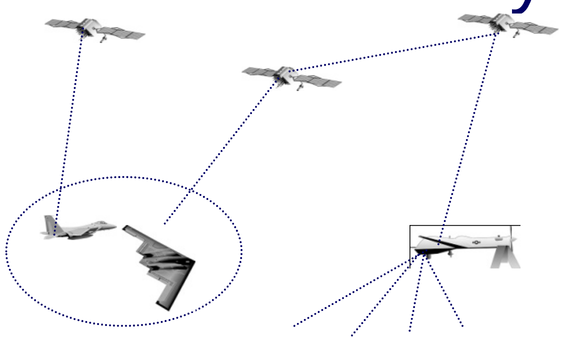
1. Important differences in context must be apparent
2. Stakeholders must be willing to share information
3. Mechanisms must exist to permit timely sharing

<u>Survivability Impact</u>: SoS constituents may be operating under incorrect or incomplete information hindering survivability

Internal Interoperability
(Ellison & Woody 2007)

Constituents in SoS must interoperate

- SoS constituents often designed and operated independently – newer constituents must interface with legacy
- Standards exist but not always enforced in SoS

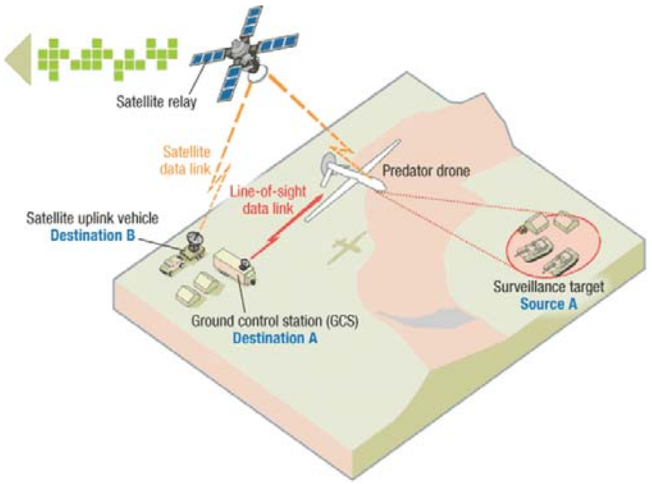


<u>Survivability Impact</u>: Weaknesses in SoS constituent interoperability may increase susceptibility, introduce vulnerabilities and inhibit timely recovery from disturbances

Dubious Validation

(Ellison & Woody 2007)

- Testing and validation of SoS difficult with evolutionary nature
- Not practical to validate each change with every permutation of past, present, and future constituents
- SoS less likely to be held to rigorous testing and validation of traditional systems



Survivability Impact: Changes in SoS constituents may hinder or enable survivability, but without testing may not be known until disturbances occur

Emerging Design Principles For Survivability

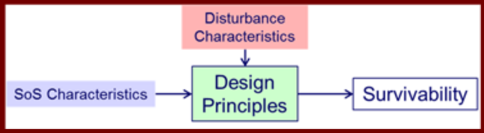
Redirection	• **Type I - Reduce Susceptibility** • Divert disturbances away from critical components • Geographical separation and component independence are enablers
Defensive Posture	• **Type I - Reduce Susceptibility** • *Be liberal in what you receive, and conservative in what you send* • Postel's Robustness Principle (1981) • May be required to address internal interoperability
Stable Intermediate Forms	• **Type II - Reduce Vulnerability** • Explicitly design for evolutionary development • Allows "fall back state" in case of disturbance • Help with validation
Adaptation	• **Type III - Increase Resilience** • System deliberately changes value delivery function by altering its form and/or CONOPs in the presence of a disturbance. • Evolutionary development and component independence are enablers.

New survivability design principles address challenges and opportunities made possible by some of the characteristics of systems of systems

Summary and Research Direction

SoS Survivability

- Characteristics of SoS
- Characteristics of disturbances
- Emerging design principles for SoS



Concept of Operations

- Need for including CONOPs in tradespace studies
- System architecture incorporates CONOPs
  - Distinguishes a system from its design

Pliability (emerging research)

- Details allowable changes in system architectures
- Provides a “guarantee” that changes won’t break system

SoS Case Scenario to Test Hypotheses

- Many SoS characteristics and subject to numerous disturbances
- Many CONOPs choices
- Hypotheses made about survivability (to be tested)