
# Design for Survivability: Concept Generation and Evaluation in Dynamic Tradespace Exploration

**2nd International Symposium on Engineering Systems**
**Cambridge, MA**
**June 17, 2009**

Matthew G. Richards, Ph.D.
*Alumnus, Engineering Systems Division*

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

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

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

Annalisa L. Weigel, Ph.D.
*Professor, Aeronautics and Astronautics & Engineering Systems*

# Agenda

- Problem Statement
- Research Questions
- Methodology Overview
- Case Application: Satellite Radar
- Discussion
- Future Work

# Problem Statement

Temporal system properties known as "ilities" (e.g., flexibility) are a critical design challenge for engineering systems

- Survivability is a critical challenge for aerospace system architecture

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 vulnerability and resilience
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 (Ross 2006)

Application of survivability methodology may address critical issue for military space

- Satellite radar architecture development

*Richards, M., Hastings, D., Rhodes, D., and Weigel, A., "Systems Architecting for Survivability: Limitations of Existing Methods for Aerospace Systems," *6th Conference on Systems Engineering Research*, Los Angeles, CA, April 2008.

# Research Questions

1. What is a dynamic, operational, and value-centric **definition** of survivability for engineering systems?

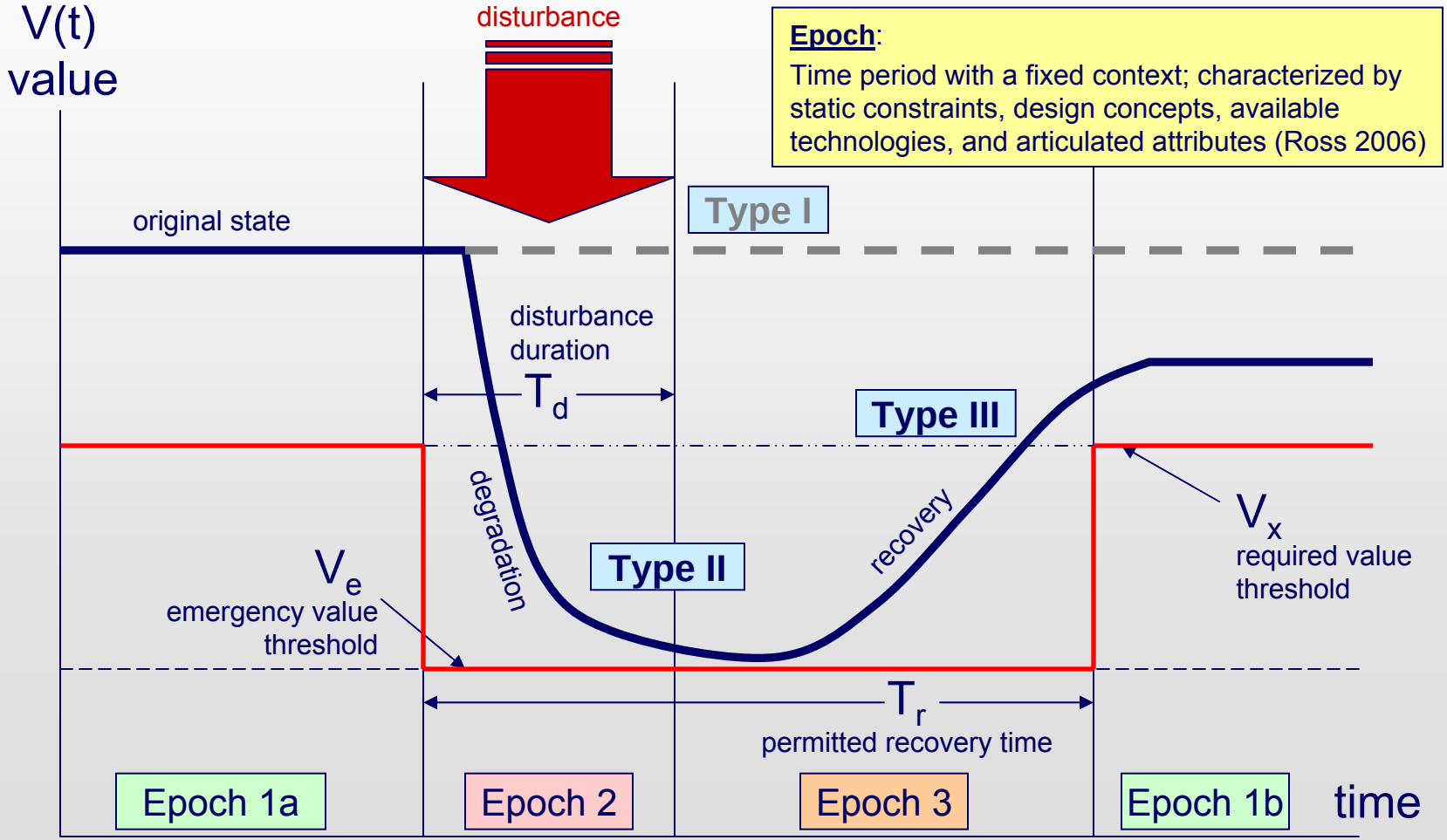
2. What **design principles** enable survivability?

3. How can survivability be quantified and used as a **decision metric in exploring tradespaces** during conceptual design of aerospace systems?

4. For a given space mission, how to **evaluate the survivability of alternative system architectures** in dynamic disturbance environments?

# 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



# Survivability Metrics

*Need to evaluate ability of system to (1) minimize utility losses and (2) meet critical value thresholds before, during, and after environmental disturbances*

**desirable attributes**: **value-based**, **dynamic**, **continuous**

## *time-weighted utility loss*

- Difference between design utility, $U_o$, and time-weighted average utility
- Internalizes lifecycle degradation
- Inspired by Quality Adjusted Life Years in health economics*

$$\overline{U}_L = U_0 - \frac{1}{T_{dl}} \cdot \int U(t)\ dt$$

$T_{dl}$ = time of design life

## *threshold availability*

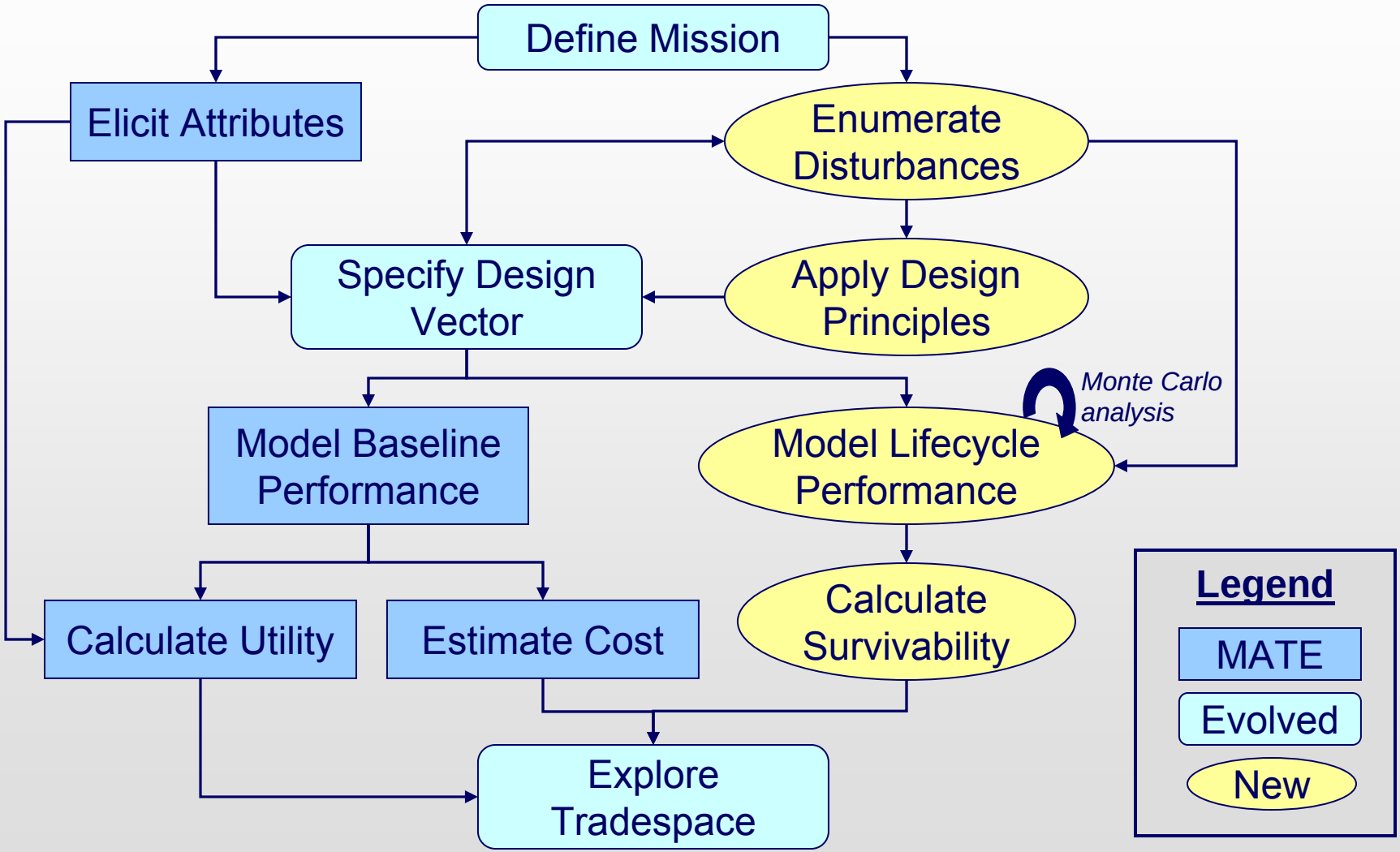
- Ratio of time above critical value thresholds ($V_x$ during baseline Epoch, $V_e$ during disturbance and recovery Epochs) to design life
- Accommodates changing expectations across contexts

$$A_T = \frac{TAT}{T_{dl}}$$

TAT = time above thresholds

*Pliskin, J., D. Shepard and M. Weinstein (1980). "Utility Functions for Life Years and Health Status." *Operations Research,* 28(1): 206-224.

# Multi-Attribute Tradespace Exploration (MATE) for Survivability

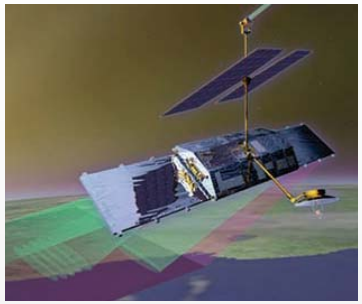


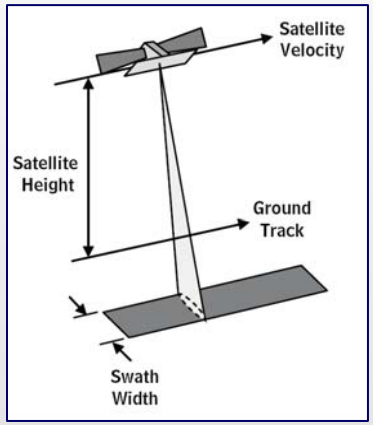
# Phases of MATE for Survivability

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
- Availability of data
  - Systems Engineering Advancement Research Initiative (SEAri)





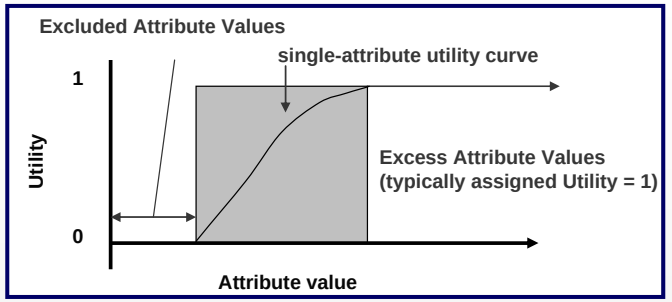

*(CBO 2007)*

**Case Application Goal**

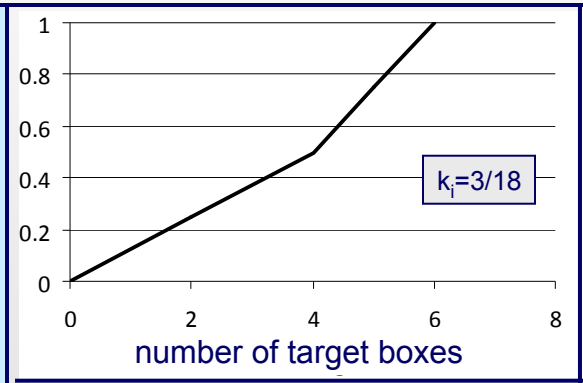
*To assess potential **satellite radar** architectures for providing the United States Military a global, all-weather, on-demand capability to **track moving ground targets**; supporting tactical military operations; maximizing cost-effectiveness; and **surviving disturbances** in the natural space environment.*

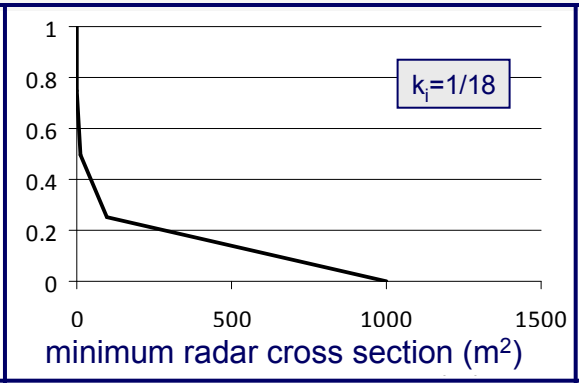
# Phase 1: Elicit Value Proposition

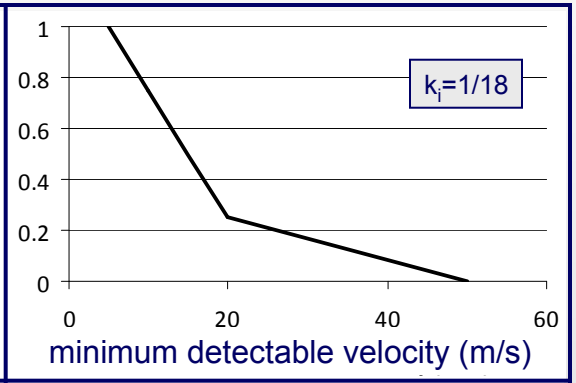
**Attributes**: *concept-neutral evaluation criteria specified by a decision maker*

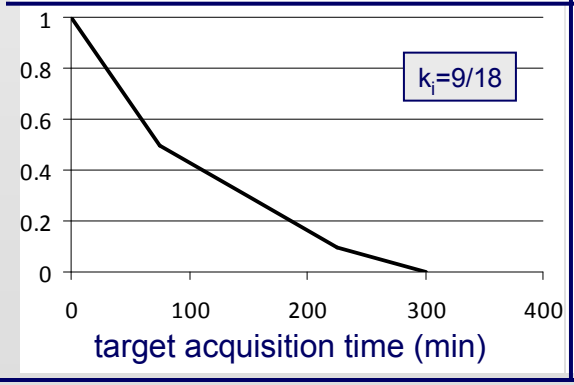


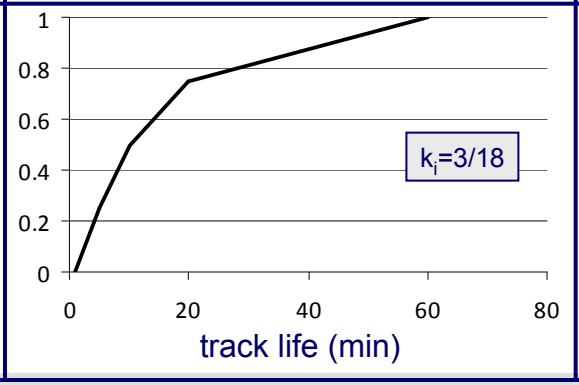

satellite radar attributes

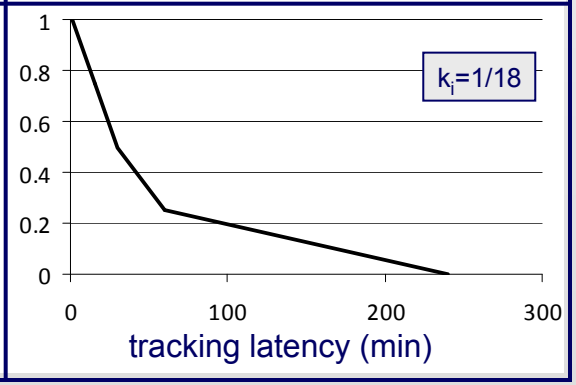


# Phase 2: Generate Concepts

*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 |
| DESIGN VARIABLES | 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 | |

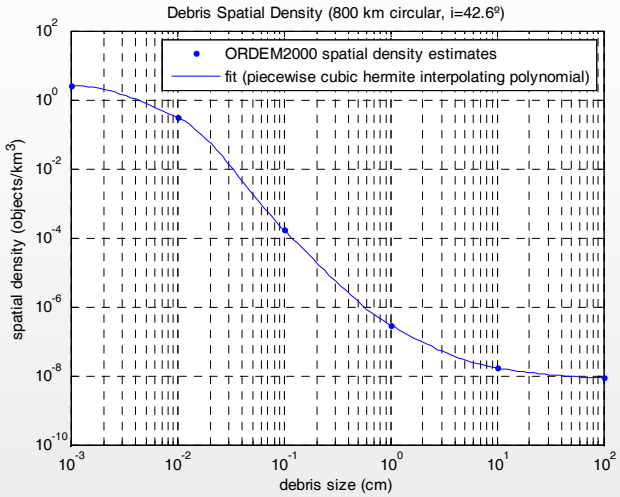
# Phase 3: Characterize Disturbance Environment

Enumerate disturbances
- Orbital debris
- Signal attenuation

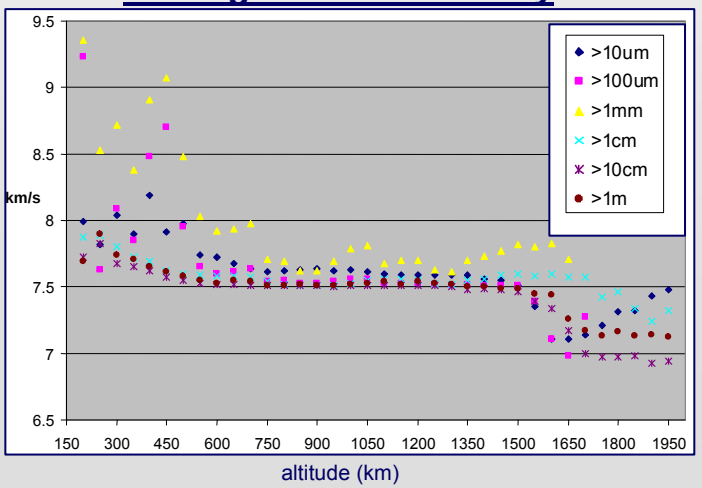
Gather data on disturbance magnitude and occurrence
- NASA ORDEM2000 debris model
  - Space Surveillance Network
  - Haystack and Haystack radar data
  - Goldstone radar data
  - Long-Duration Exposure Facility
  - Hubble Telescope array impact data
  - Space Shuttle impact data
  - Mir impact data

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*

| | 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 |

***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 |

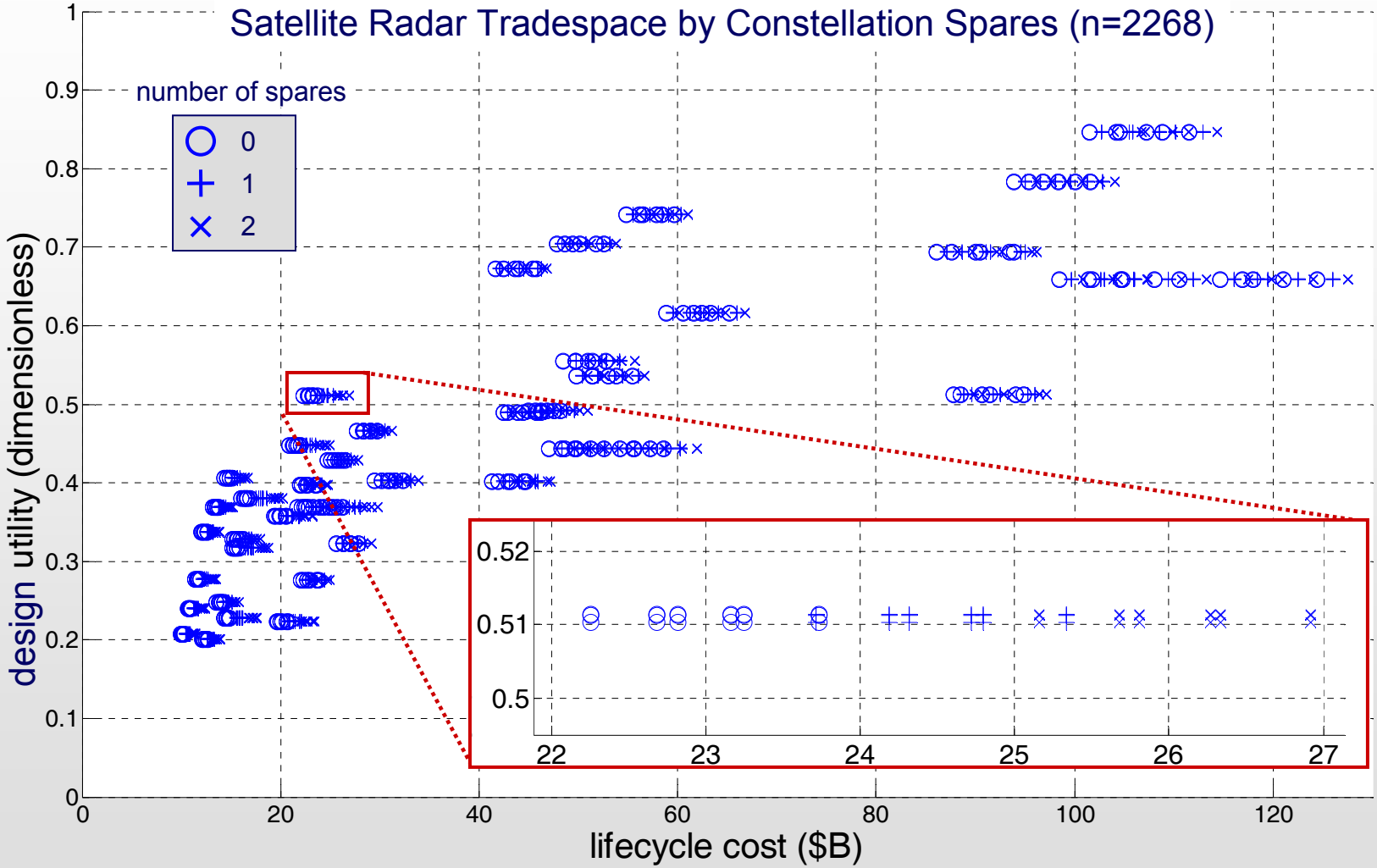
| Comm. Architecture |
|---|
| Direct Downlink Only |
| Relay Backbone |

survivability variables

| Constellation Spares |
|---|
| 0 |
| 1 |
| 2 |

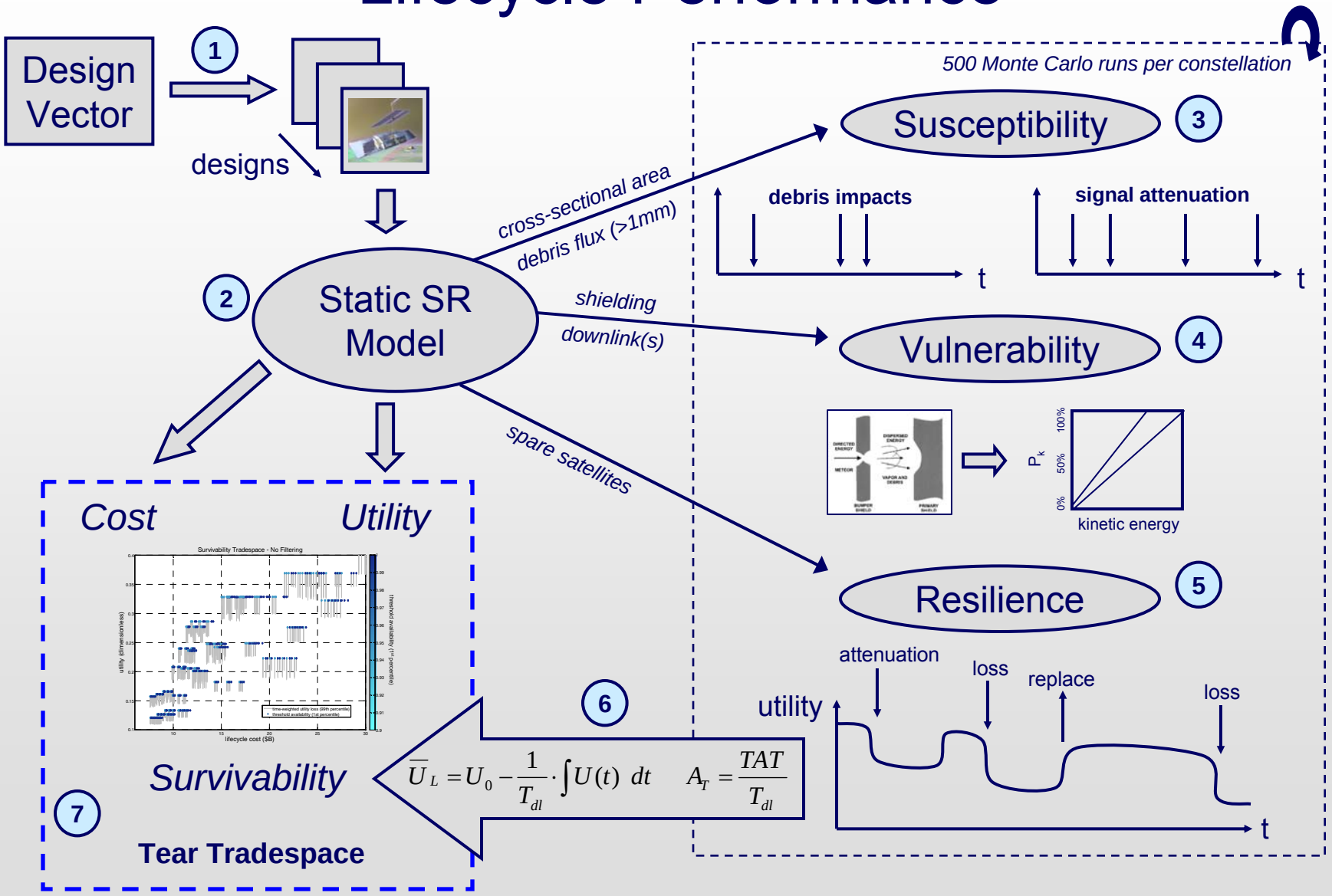
| Shield Thickness (mm) |
|---|
| 1 |
| 5 |
| 10 |

# Phase 5: Model Baseline System Performance

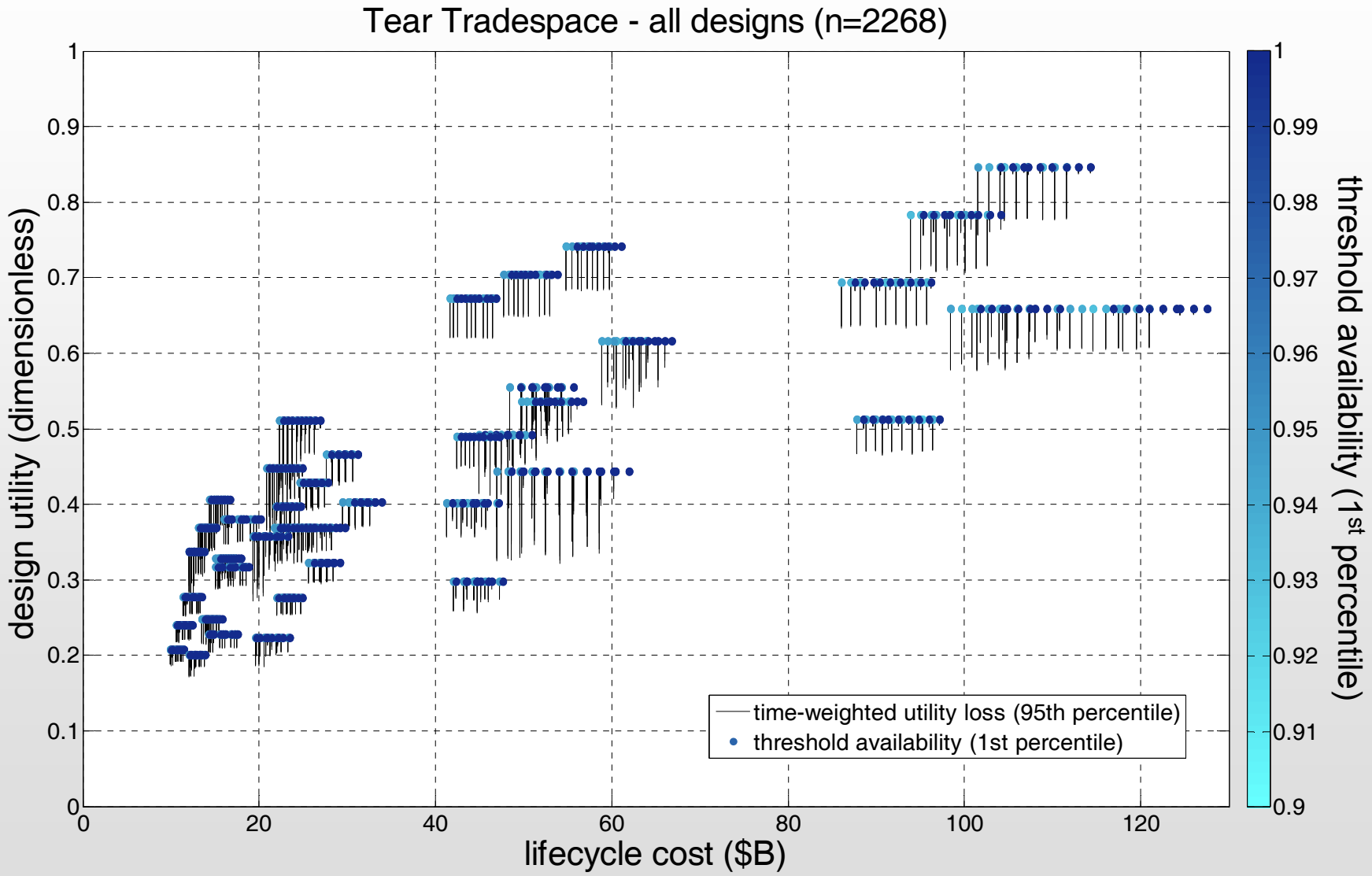



*Baseline tradespace only internalizes costs of survivability features*

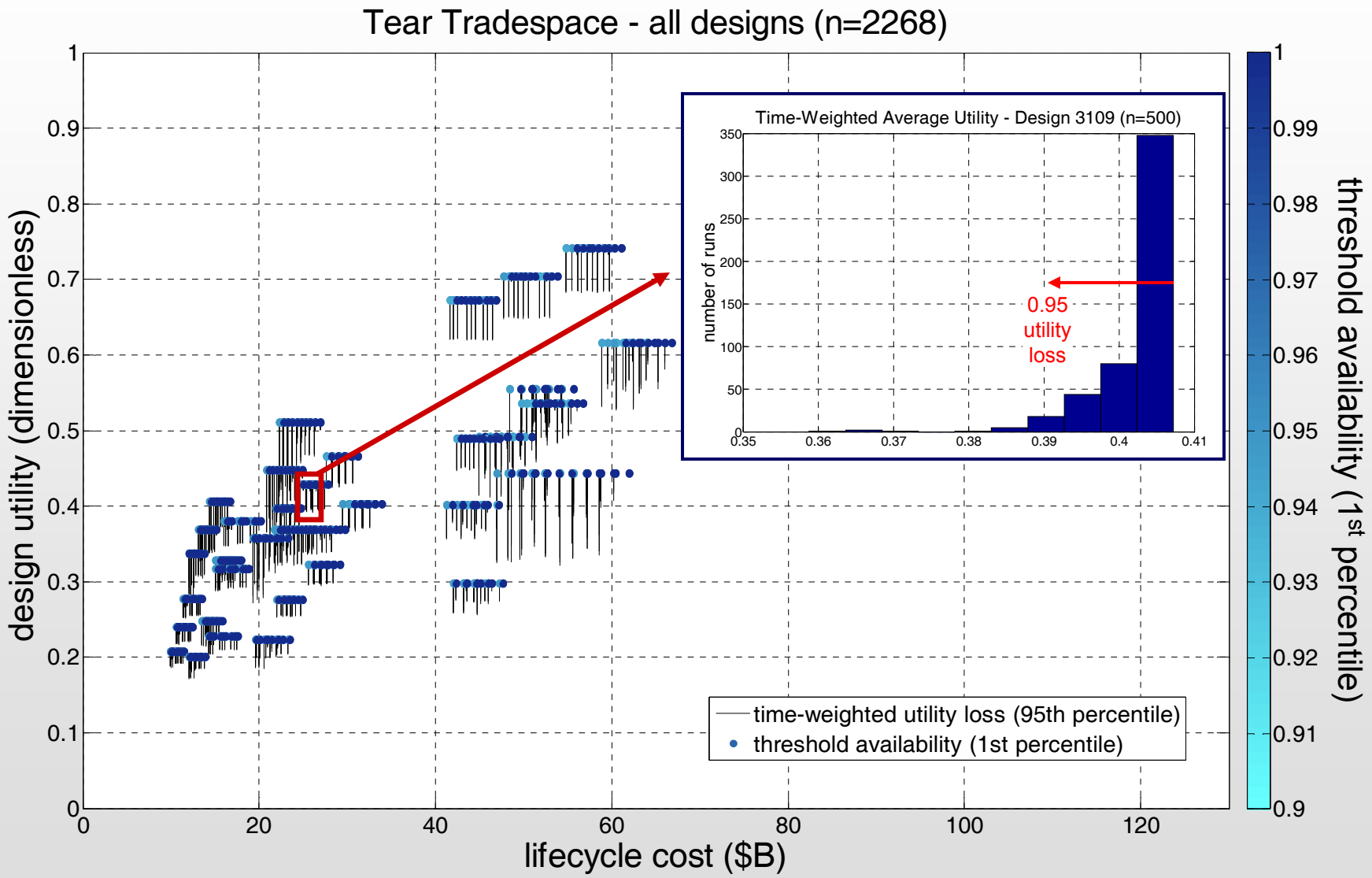
# Phase 6: Model Impact of Disturbances on Lifecycle Performance



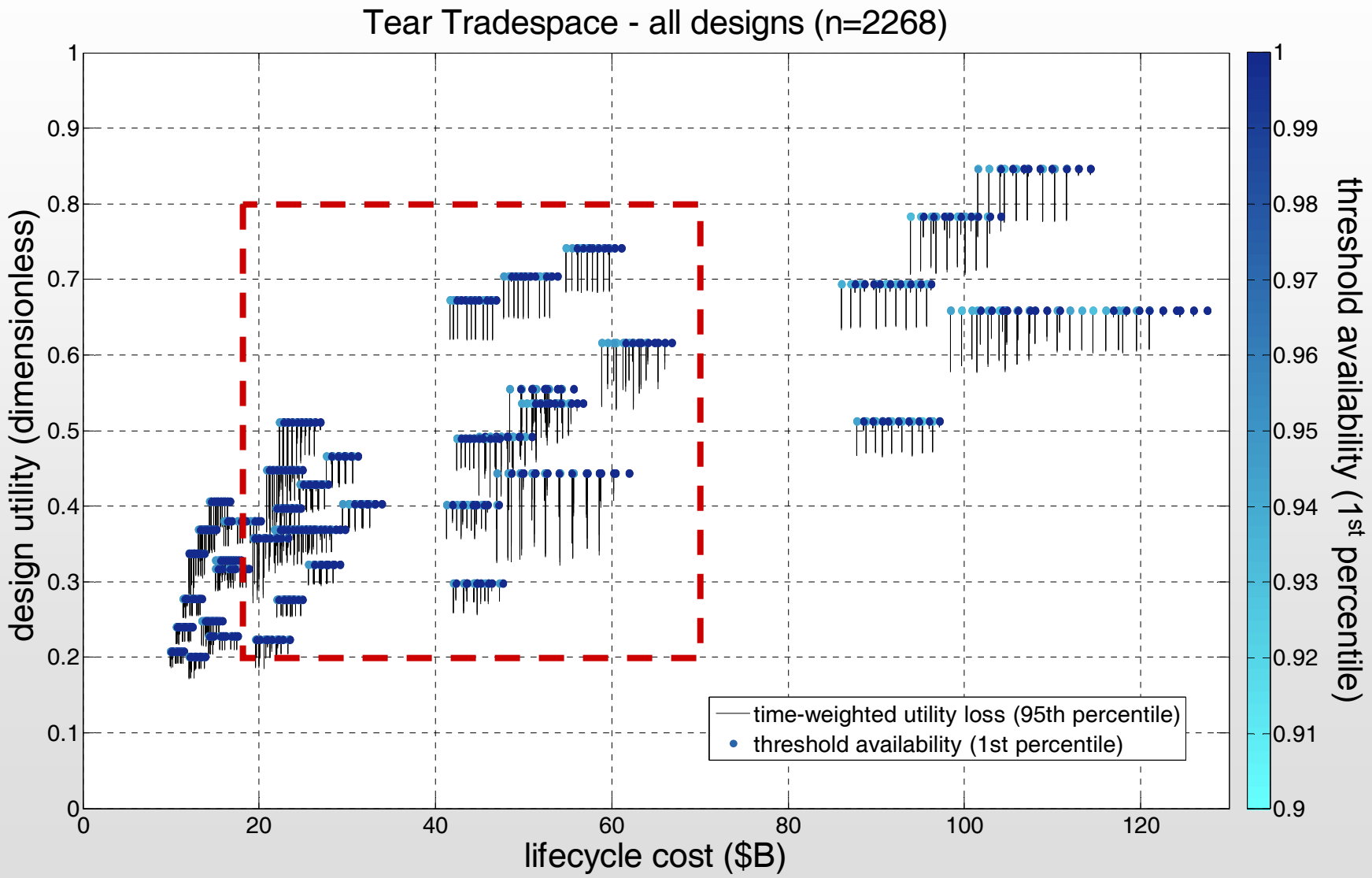
# Phase 7: Apply Survivability Metrics



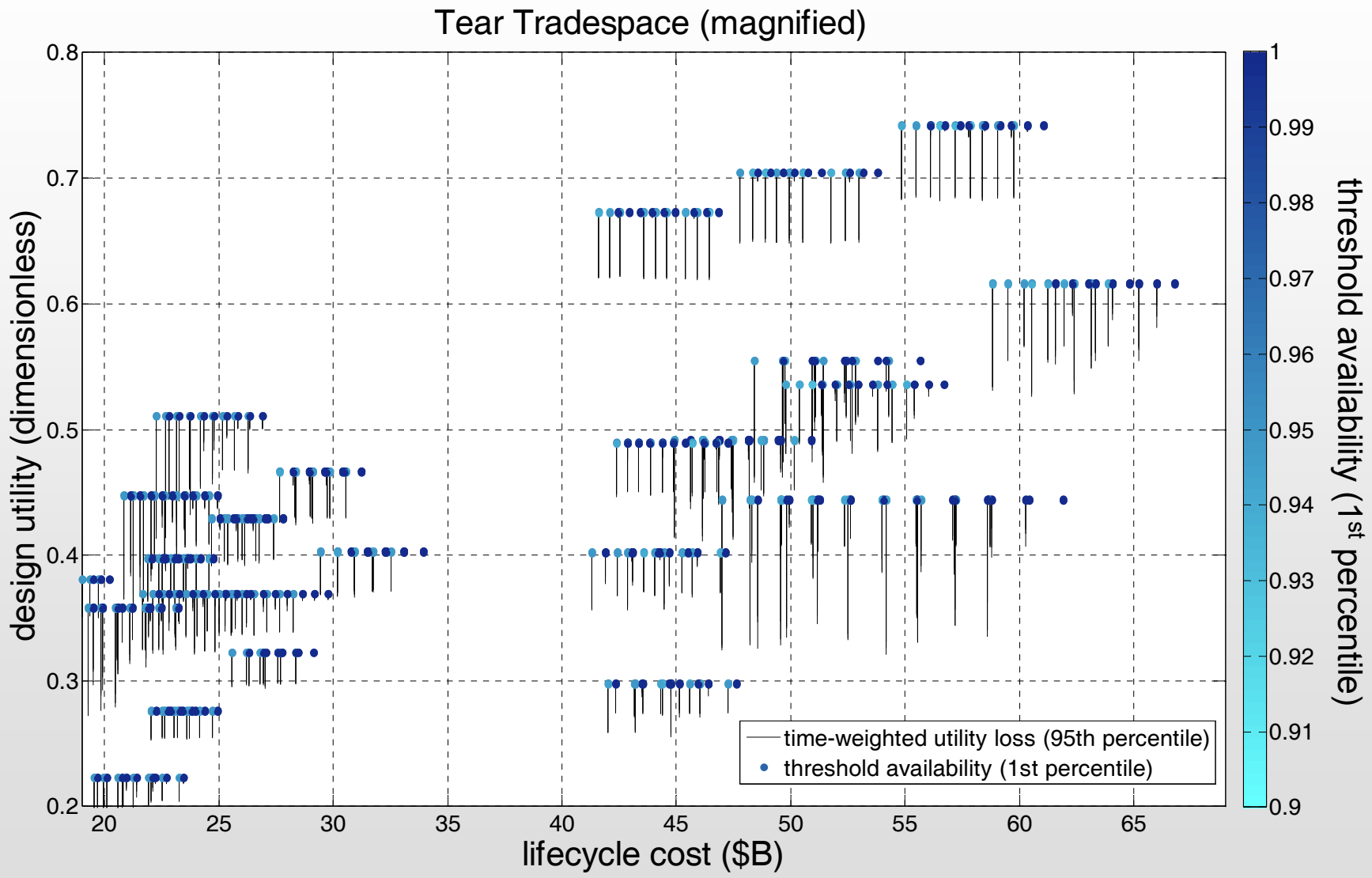
# Phase 7: Apply Survivability Metrics



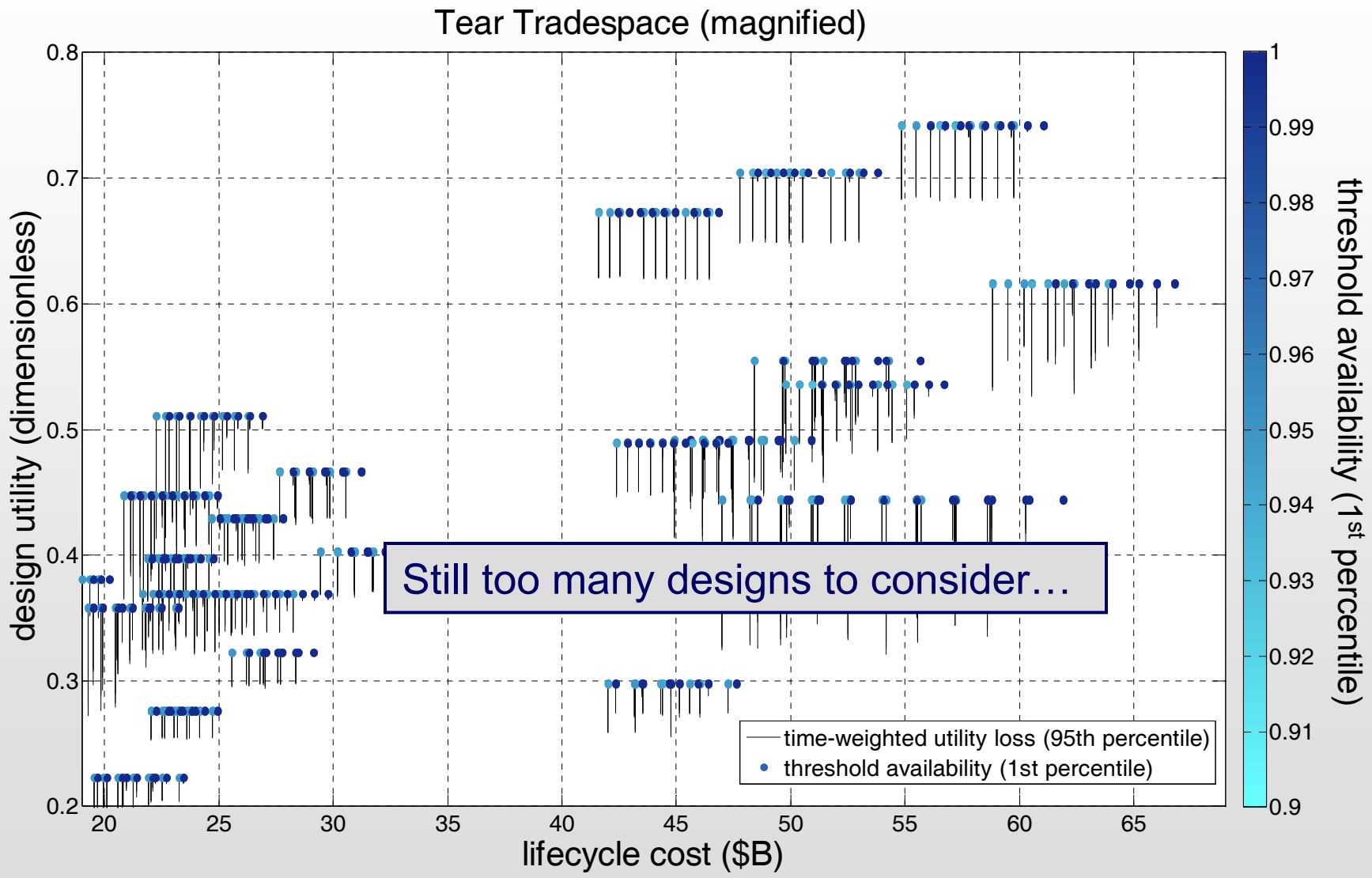
# Phase 8: Explore Tradespace



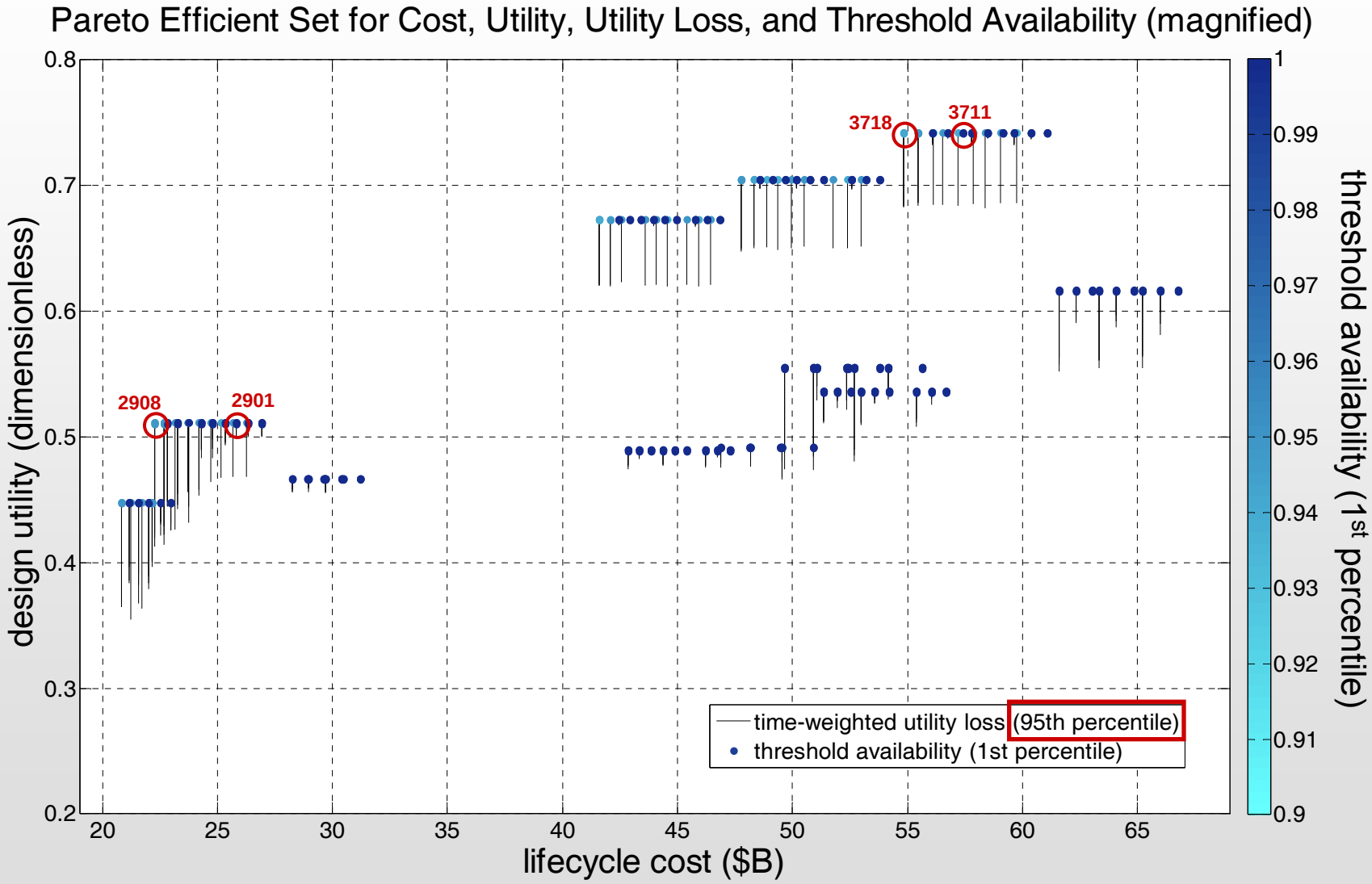
# Magnify Tear Tradespace



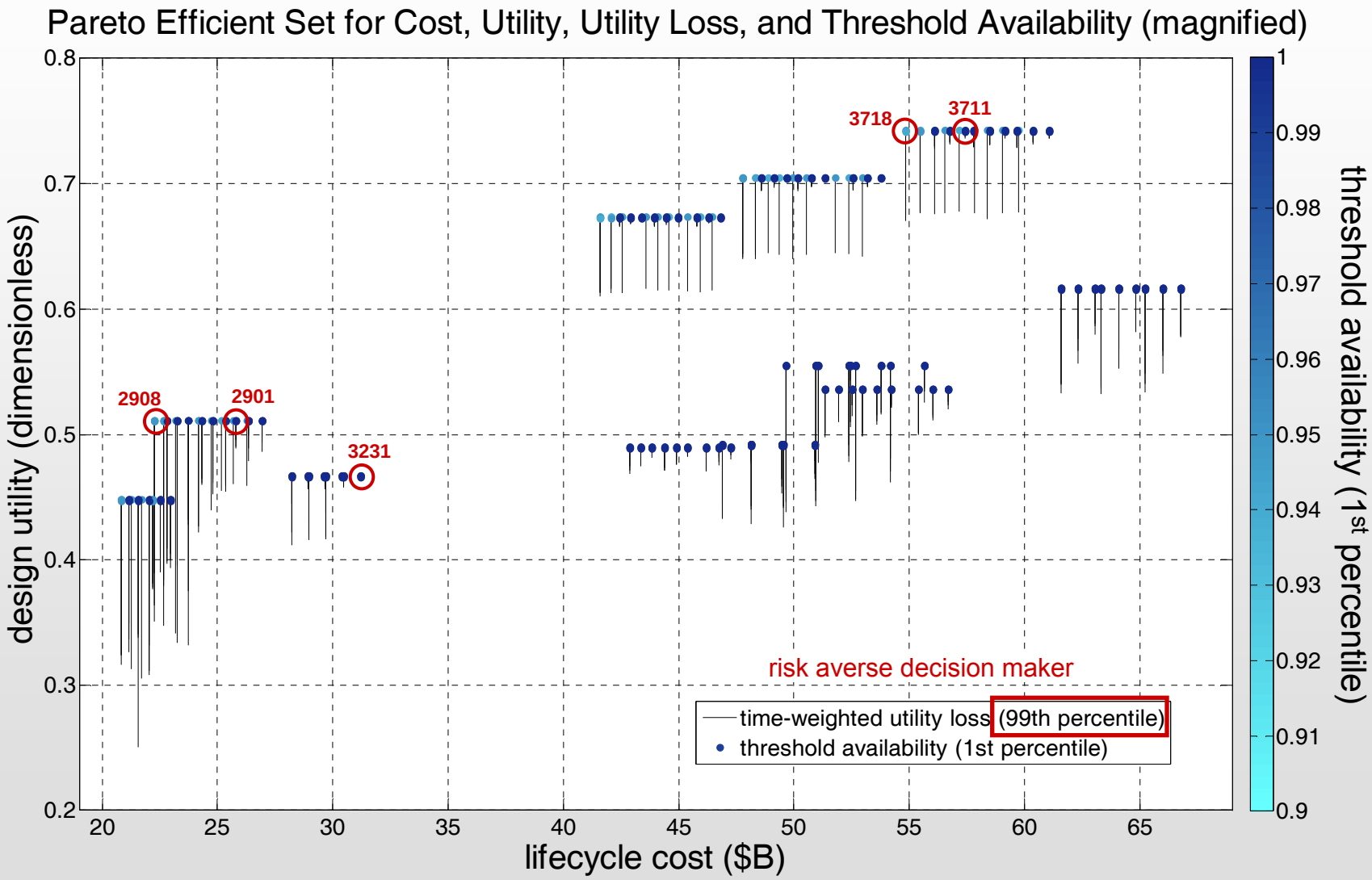
# Magnify Tear Tradespace



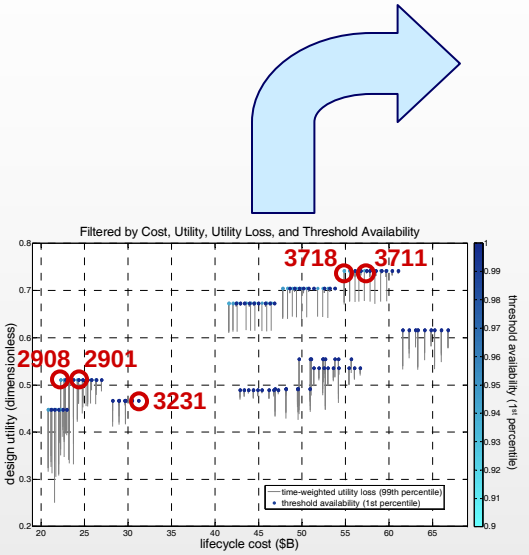
# Identify Pareto-Efficient Surface of Cost, Utility, and Survivability



# Select Interesting Point Designs



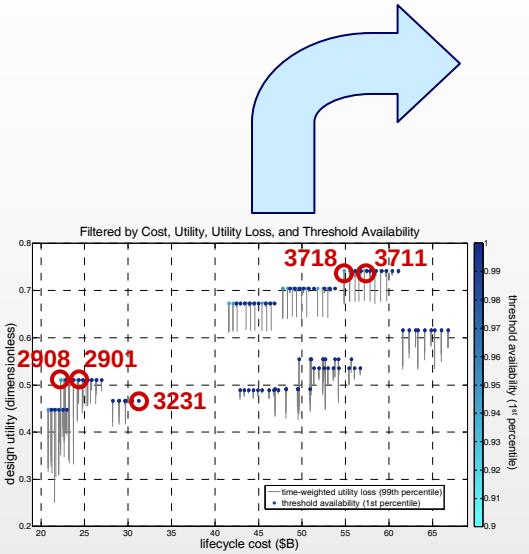
# Extract Survivability Insights from Selected Point Designs




| Design Vector ID | 2908 | 2901 | 3231 | 3718 | 3711 |
|---|---|---|---|---|---|
| orbit altitude (km) | 1500 | | | 1500 | |
| Walker constellation | 9/3/2 | 9/3/2 | 27/3/1 | 66/6/5 | 66/6/5 |
| transmit frequency (GHz) | 10 | | | 10 | |
| antenna area (m^2) | 100 | 100 | 40 | 40 | |
| antenna type | AESA | | | AESA | |
| radar bandwidth (MHz) | 2000 | | | 2000 | |
| peak transmit power (kW) | 20 | | | 20 | |
| tugable | no | | | no | |
| comm. architecture | direct | relay | relay | direct | relay |
| tactical link | yes | | | yes | |
| shield thickness (mm) | 1 | 1 | 10 | 1 | |
| satellite spares | 0 | 2 | 2 | 0 | 2 |
| lifecycle cost ($B) | 22.3 | 25.8 | 31.2 | 54.8 | 57.4 |
| utility | 0.51 | 0.51 | 0.47 | 0.74 | 0.74 |
| utility loss (95th) | 0.09 | 0.01 | 0.00 | 0.06 | 0.00 |
| utility loss (99th) | 0.12 | 0.02 | 0.00 | 0.07 | 0.01 |
| threshold availability (1st) | 0.95 | 1.00 | 1.00 | 0.95 | 1.00 |

- Survivability insights from selected point designs
  - Relay backbone critical for achieving continuous threshold availability
  - Investing in spare satellite(s) minimizes utility losses
  - Satellite shielding has limited impact in nominal debris environment
  - Distributed constellation mitigates worst-case risks

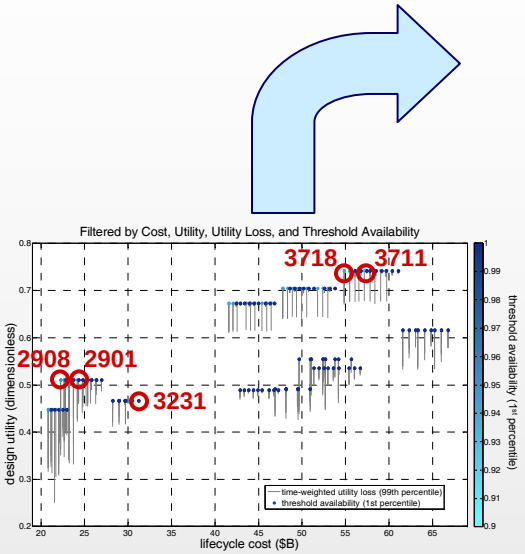
# Extract Survivability Insights from Selected Point Designs




| Design Vector ID | 2908 | 2901 | 3231 | 3718 | 3711 |
|---|---|---|---|---|---|
| orbit altitude (km) | 1500 | | | 1500 | |
| Walker constellation | 9/3/2 | 9/3/2 | 27/3/1 | 66/6/5 | 66/6/5 |
| transmit frequency (GHz) | 10 | | | 10 | |
| antenna area (m^2) | 100 | 100 | 40 | 40 | |
| antenna type | AESA | | | AESA | |
| radar bandwidth (MHz) | 2000 | | | 2000 | |
| peak transmit power (kW) | 20 | | | 20 | |
| tugable | no | | | no | |
| comm. architecture | direct | relay | relay | direct | relay |
| tactical link | yes | | | yes | |
| shield thickness (mm) | 1 | 1 | 10 | 1 | |
| satellite spares | 0 | 2 | 2 | 0 | 2 |
| lifecycle cost ($B) | 22.3 | 25.8 | 31.2 | 54.8 | 57.4 |
| utility | 0.51 | 0.51 | 0.47 | 0.74 | 0.74 |
| utility loss (95th) | 0.09 | 0.01 | 0.00 | 0.06 | 0.00 |
| utility loss (99th) | 0.12 | 0.02 | 0.00 | 0.07 | 0.01 |
| threshold availability (1st) | 0.95 | 1.00 | 1.00 | 0.95 | 1.00 |

- Survivability insights from selected point designs
  - Relay backbone critical for achieving continuous threshold availability
  - Investing in spare satellite(s) minimizes utility losses
  - Satellite shielding has limited impact in nominal debris environment
  - Distributed constellation mitigates worst-case risks

# Extract Survivability Insights from Selected Point Designs




| Design Vector ID | 2908 | 2901 | 3231 | 3718 | 3711 |
|---|---|---|---|---|---|
| orbit altitude (km) | 1500 | | | 1500 | |
| Walker constellation | 9/3/2 | 9/3/2 | 27/3/1 | 66/6/5 | 66/6/5 |
| transmit frequency (GHz) | 10 | | | 10 | |
| antenna area (m^2) | 100 | 100 | 40 | 40 | |
| antenna type | AESA | | | AESA | |
| radar bandwidth (MHz) | 2000 | | | 2000 | |
| peak transmit power (kW) | 20 | | | 20 | |
| tugable | no | | | no | |
| comm. architecture | direct | relay | relay | direct | relay |
| tactical link | yes | | | yes | |
| shield thickness (mm) | 1 | 1 | 10 | 1 | |
| satellite spares | 0 | 2 | 2 | 0 | 2 |
| lifecycle cost ($B) | 22.3 | 25.8 | 31.2 | 54.8 | 57.4 |
| utility | 0.51 | 0.51 | 0.47 | 0.74 | 0.74 |
| utility loss (95th) | 0.09 | 0.01 | 0.00 | 0.06 | 0.00 |
| utility loss (99th) | 0.12 | 0.02 | 0.00 | 0.07 | 0.01 |
| threshold availability (1st) | 0.95 | 1.00 | 1.00 | 0.95 | 1.00 |

- Survivability insights from selected point designs
  - Relay backbone critical for achieving continuous threshold availability
  - Investing in spare satellite(s) minimizes utility losses
  - Satellite shielding has limited impact in nominal debris environment
  - Distributed constellation mitigates worst-case risks

# Methodological Insights

MATE 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 design alternatives

Implementation considerations

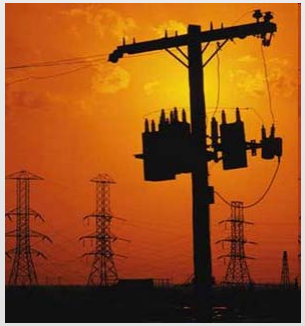
- Subject percentile reporting levels to sensitivity analysis
- Balance broad exploration with selected of individual point designs

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

- Pareto front in traditional MATE study excludes most survivable designs
- Evaluates survivability implications for selection of baseline architecture

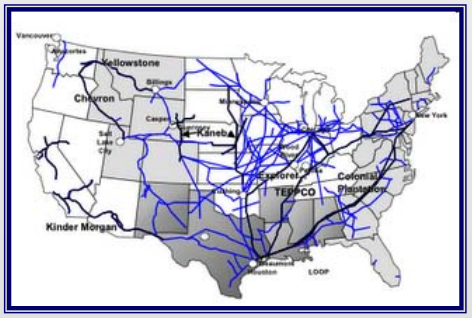
# Future Work

- 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

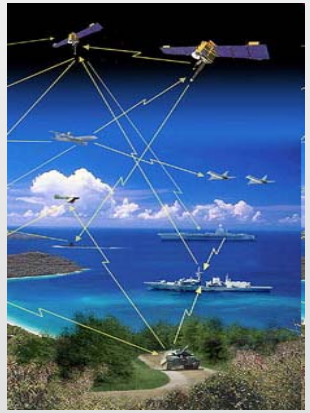


*power distribution*

*transportation*




*water distribution*



*communications*


# Questions?

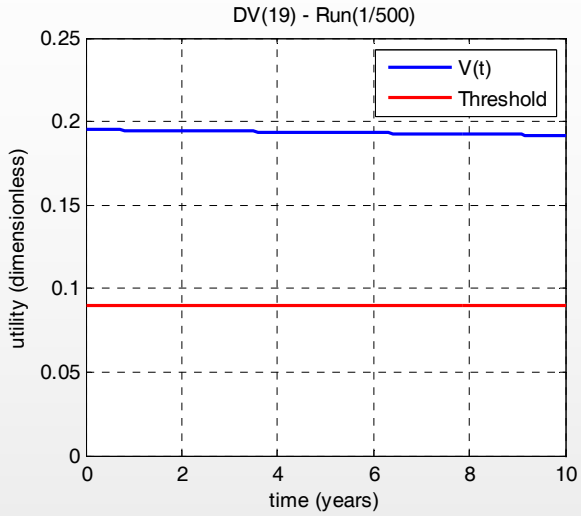
Matthew Richards, Ph.D.
mgr@alum.mit.edu

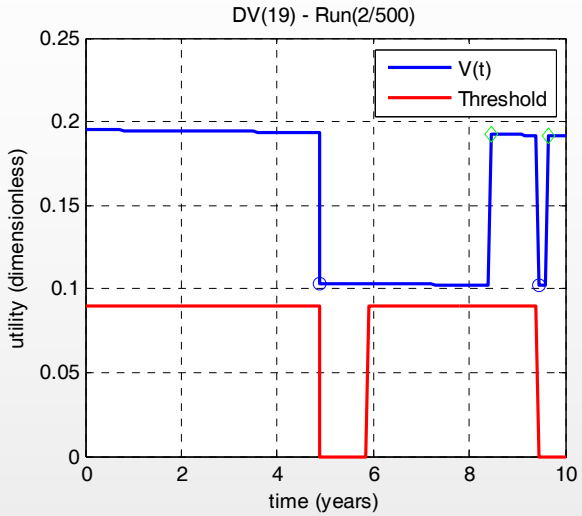
# Limitations of Existing Metrics

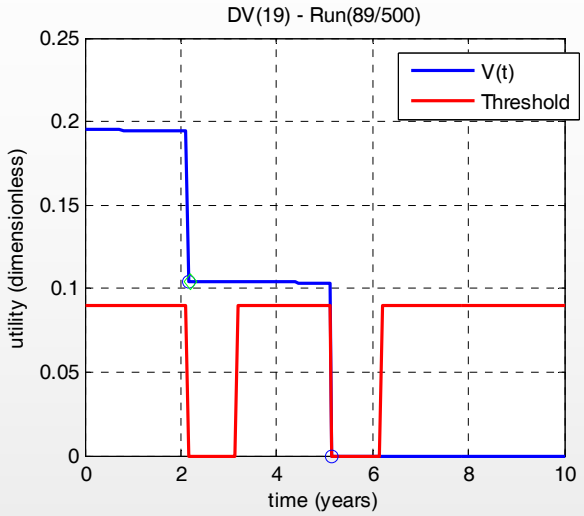
| | | |
|---|---|---|
| Engagement Survivability | $P_S = 1 - P_K = 1 - P_H \cdot P_{K/H}$<br>S = survive, K = kill, H = hit | • Binary assessment criteria fails to internalize graceful degradation |
| Campaign Survivability | $CS = (P_S)^N = (1 - P_K)^N$<br>N = number of engagements | • Binary assessment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

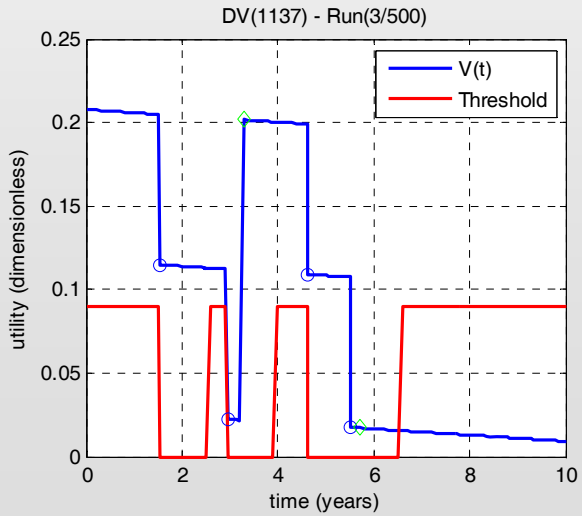
*(Ball 2003; Blanchard and Fabrycky 2006)*

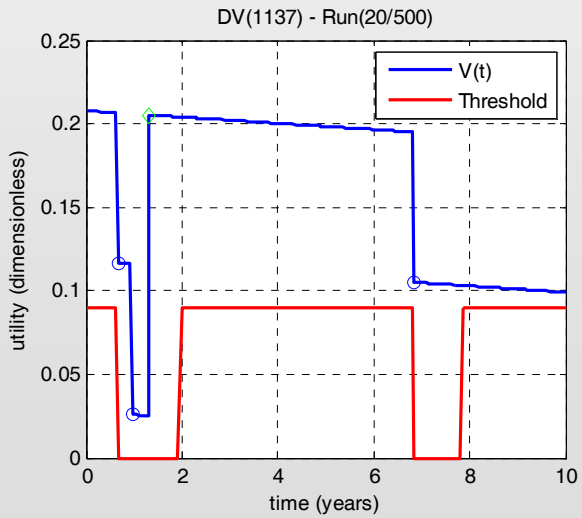
# Need Measures of Central Tendency Across Runs

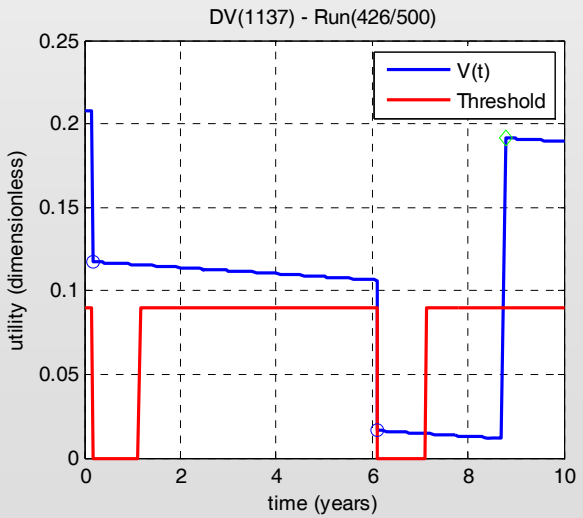


# General Conclusions

- Definition of baseline system architecture should include survivability considerations for efficient mitigation of disturbances
- 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
- Conceptualization of survivability for engineering systems is a ***solution-generating*** and ***decision-making*** framework, enabling discovery of systems robust to finite-duration disturbances