SEA RI
Systems Engineering Advancement
Research Initiative

DRAPER
LABORATORY

Application of Epoch-Era Analysis to the Design of Engineered Resilient Systems

Case Study on Earth Imaging Satellite Constellations

Mike Curry

October 30, 2014

Outline

- Motivation
- Traditional Tradespace Exploration
  - Point Designs
  - Pareto Frontier
  - Full Tradespace
  - Optimization
- Defining Resilience
- Epoch-Era Analysis
- Resilience in Space Systems
- Case Study
  - Overview
  - Tradespace Exploration
  - Multi-Epoch Results
  - Multi-Era Results
- Summary / Future Work

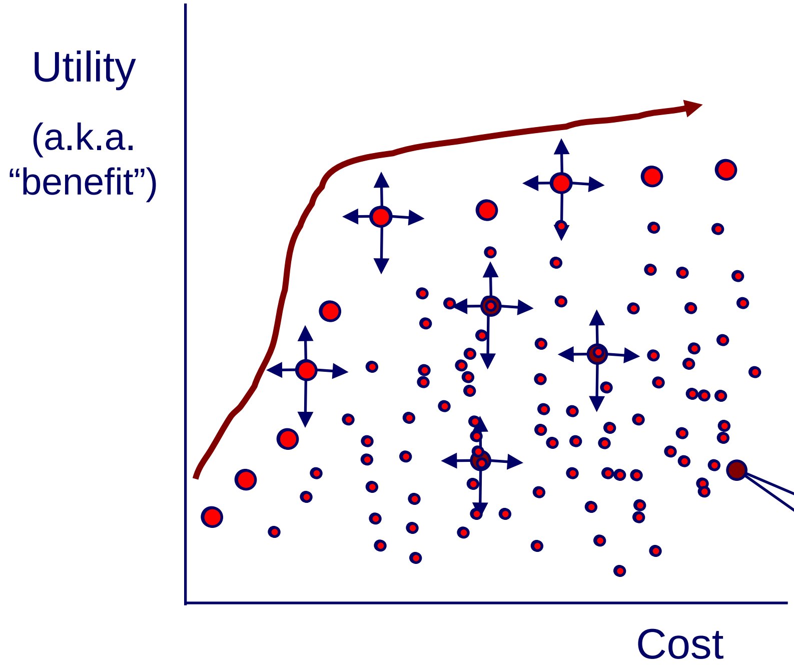
Motivation for Resilient Space Systems

- Uncertain Futures: technology, competitors and mission needs change before system is even completed
- Increasing Complexity: complexity growing over time, not only due to scale and interconnectedness, but also due to increased scope in our ability to describe the system[1]

- Space systems are particular susceptible to these issues
  - **Long development times**: adversary timescales shorter than system lifecycle
  - **Long lifecycles** make it difficult to capitalize on new technologies or adapt to changing threats and needs
- Typical conceptual design approaches focus on optimizing performance for a nominal context and set of stakeholder needs

"Our spacecraft, which take 5 to 10 years to build, and then last up to 20 … will be configured to solve tomorrow's problems using yesterday's technologies."
Dr. Owen Brown, DARPA Program Manager, 2007

Tradespace Exploration
Exploring Tradeoffs between “Choices”



Design$_i$ = {X$_1$, X$_2$, X$_3$,…,X$_j$}

Differing types of “trades”

0. Choose a solution

1. Local point solution trades

2. Multiple points with trades

3. Frontier solution set

4. Full tradespace exploration

Tradespace exploration enables big picture understanding of the current problem

Need for Anticipatory Capacity

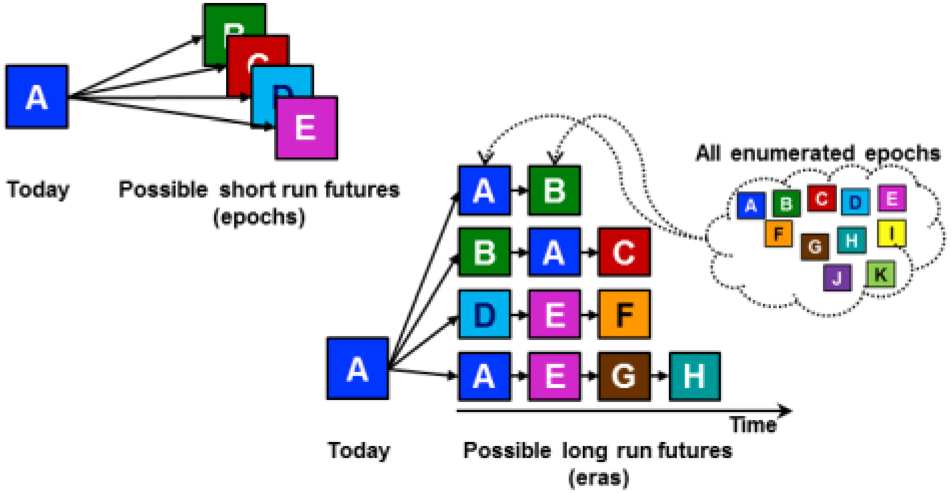
> Engineering "involves a relation among three terms: the **purpose** or goal, the character of the **artifact**, and the **environment** in which the artifact performs"
>
> \- Herb Simon, *The Science of the Artificial*, MIT Press: Cambridge, 1996

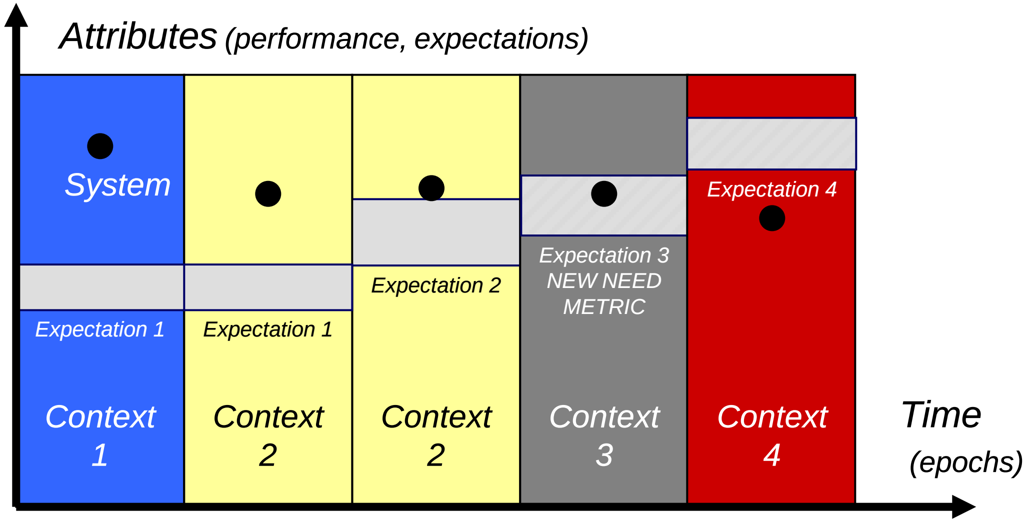
- Tradespace exploration doesn't consider the dynamic nature of the value delivery of the system
- Changes in system / context / needs impact the value proposition and thus the "success" of the system
- Epoch-Era Analysis allows for explicit consideration of the impacts of changes in system / context / needs

- System
  - Degradation / malfunctions
  - Software updates and retrofits
- Needs / Expectations
  - Requirements change
  - Mission change
- Context / Environment
  - Political / Legal / Regulatory
  - Economic
  - Social
  - Technological
  - Environmental

Epoch-Era Analysis (EEA)

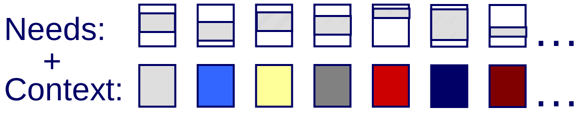
- Conceptualizes the effects of time and changing context on a system[5,6]
  - Epochs: periods of fixed context and needs (short run)
  - Eras: sequences of epochs simulating a potential future lifecycle path experienced by the system (long run)





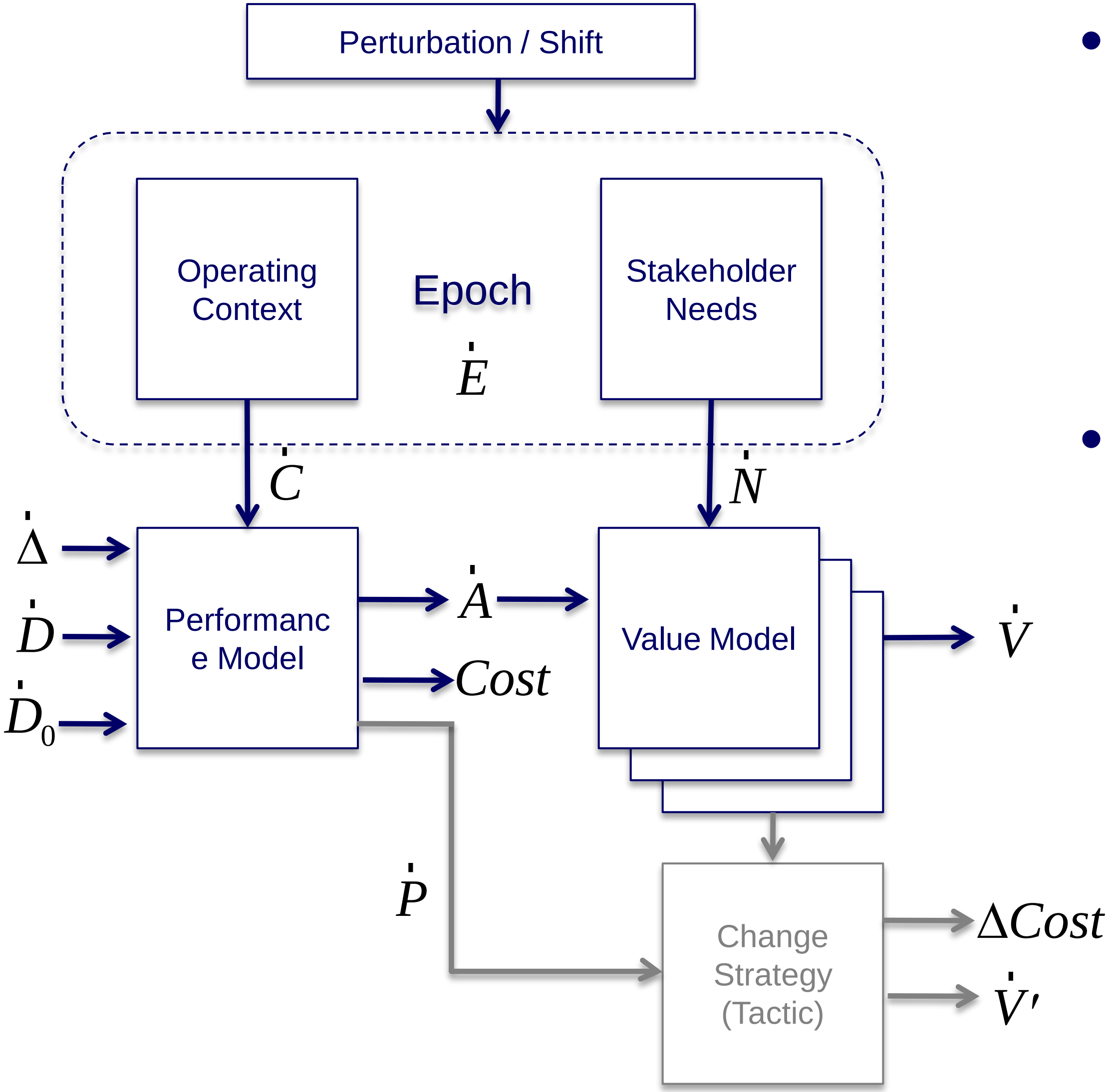
Two aspects to an ***Epoch***:

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



EEA is a framework that supports narrative and computational scenario planning and analysis for both short and long run futures[7]

Tradespace Exploration vs EEA



- Tradespace Exploration tends to focus on system alternatives within a static context and needs
- EEA explicitly considers the dynamic environment in which the system will need to sustain value delivery to its stakeholders

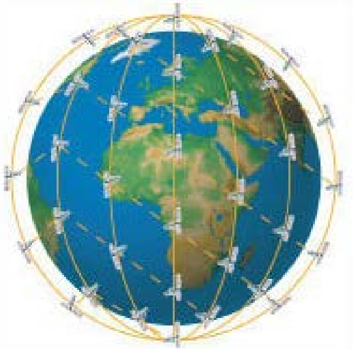
Defining Resilience

- Ability of a system to offer broad utility in a wide range of operations across many potential alternative futures despite experiencing disruptions [Neches & Madni, 2012]

- Ability of a system to circumvent, survive, and recover from failures to ultimately achieve mission objectives. A resilient system is able to reason about own/environmental states in the presence of environmental uncertainty [Madni, 2012]

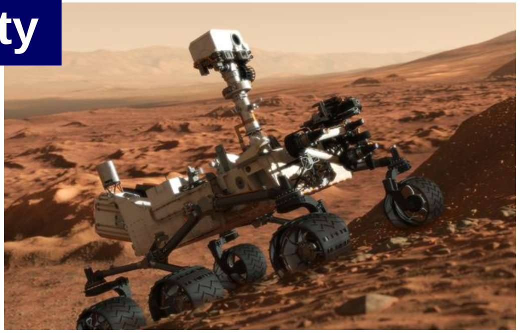
- Ability of a system to minimize the impact of a finite-duration disturbance on value delivery through (1) the reduction of the likelihood or magnitude of a disturbance, (2) the satisfaction of a minimally acceptable level of value delivery during and after a disturbance, (3) timely recovery [Richards et. al, 2007]

Iridium



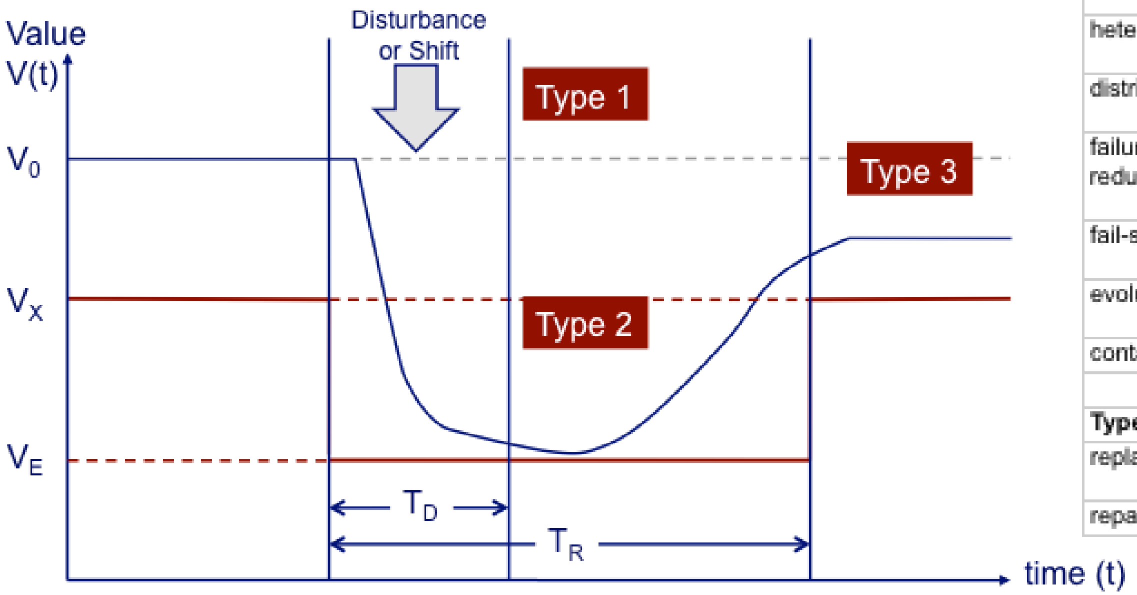
Hubble

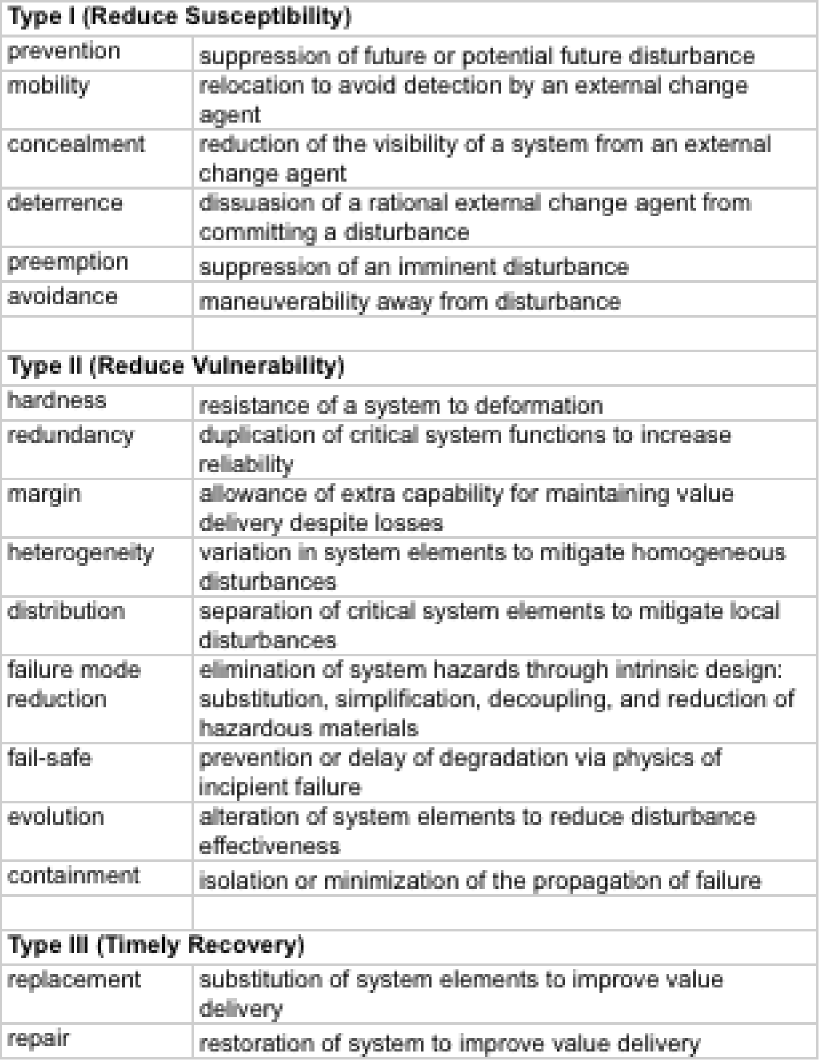
Curiosity



Defining Value Sustainment
(aka Resilience / Survivability)

Ability of a system to minimize the impact of a finite-duration disturbance on value delivery through (1) the reduction of the likelihood or magnitude of a disturbance, (2) the satisfaction of a minimally acceptable level of value delivery during and after a disturbance, (3) timely recovery [Richards et al, 2007]

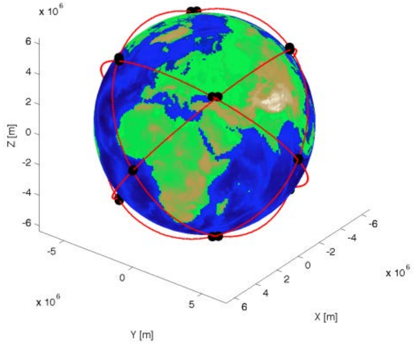




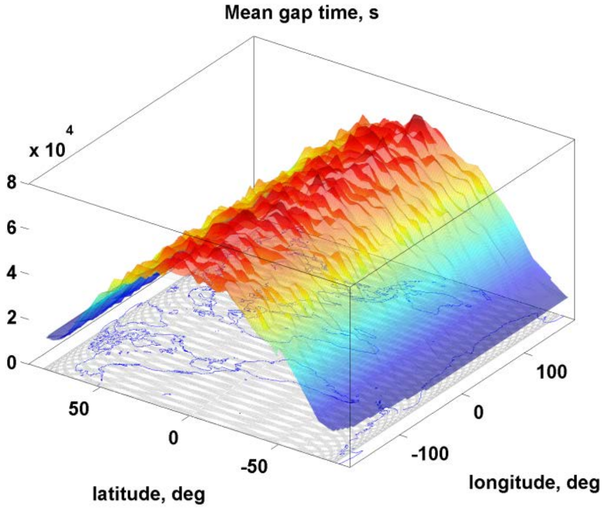
Type I (Reduce Susceptibility)	
prevention	suppression of future or potential future disturbance
mobility	relocation to avoid detection by an external change agent
concealment	reduction of the visibility of a system from an external change agent
deterrence	dissuasion of a rational external change agent from committing a disturbance
preemption	suppression of an imminent disturbance
avoidance	maneuverability away from disturbance
Type II (Reduce Vulnerability)	
hardness	resistance of a system to deformation
redundancy	duplication of critical system functions to increase reliability
margin	allowance of extra capability for maintaining value delivery despite losses
heterogeneity	variation in system elements to mitigate homogeneous disturbances
distribution	separation of critical system elements to mitigate local disturbances
failure mode reduction	elimination of system hazards through intrinsic design: substitution, simplification, decoupling, and reduction of hazardous materials
fail-safe	prevention or delay of degradation via physics of incipient failure
evolution	alteration of system elements to reduce disturbance effectiveness
containment	isolation or minimization of the propagation of failure
Type III (Timely Recovery)	
replacement	substitution of system elements to improve value delivery
repair	restoration of system to improve value delivery

Case Study: Earth Imaging Satellites

- Imaging of the Earth's surface is a desired capability for many applications and problem domains
  - Military surveillance
  - Commercial applications
  - Earth Science applications
  - Agriculture / Forestry

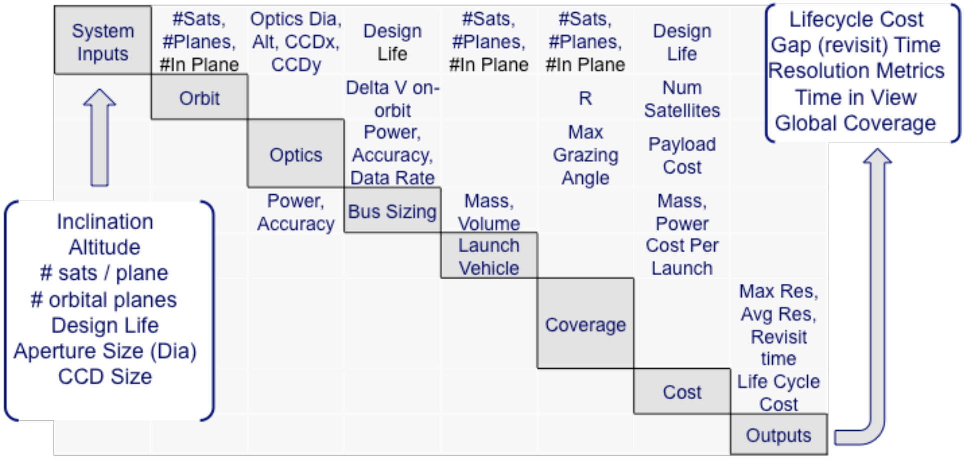


- Problem Statement: *To provide* ***affordable, low-latency, high-resolution, near-continuous*** *imaging of an* ***arbitrary location*** *on the Earth's surface*
- **Mapping of Problem Statement to Objectives:**
  - Minimize lifecycle cost (***affordable***)
  - Minimize gap / revisit time (***low-latency***)
  - Minimize resolution (m/pixel) (***high-resolution***)
  - Maximize time in view (***near-continuous***)
  - Maximize global coverage (***arbitrary location***)



Performance and Value Models

- Performance Models
  - Integrated models for orbits, bus sizing, optical coverage map design vector onto performance attributes
  - Lifecycle Cost model considers R&D, first-unit, manufacturing, launch and operations costs



System Inputs	#Sats, #Planes, #In Plane	Optics Dia, Alt, CCDx, CCDy	Design Life	#Sats, #Planes, #In Plane	#Sats, #Planes, #In Plane	Design Life	
	Orbit		Delta V on-orbit		R	Num Satellites	
		Optics	Power, Accuracy, Data Rate		Max Grazing Angle	Payload Cost	
		Power, Accuracy	Bus Sizing	Mass, Volume		Mass, Power	
				Launch Vehicle		Cost Per Launch	
					Coverage		Max Res, Avg Res, Revisit time
						Cost	Life Cycle Cost
							Outputs

Inclination
Altitude
# sats / plane
# orbital planes
Design Life
Aperture Size (Dia)
CCD Size

Lifecycle Cost
Gap (revisit) Time
Resolution Metrics
Time in View
Global Coverage

$$\|J_i\| = \frac{J_i - J_{nadir}}{J_{utopia} - J_{nadir}}$$

$$Cost = \|J_1\|$$

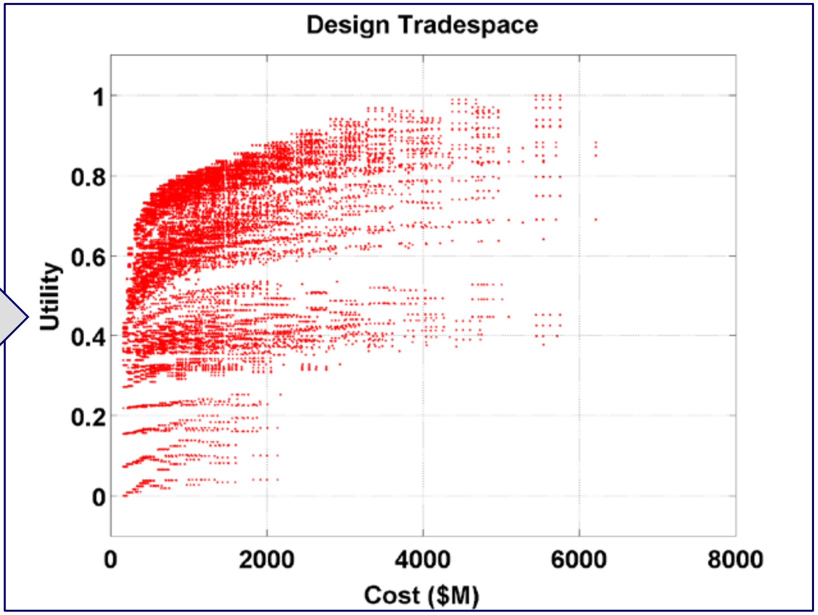
$$U = \sum_{i=2}^{6} w_i \|J_i\|, \quad w_i = 0.2 \quad (i = 2,\ldots,6)$$

- Utility Theory applied to convert the attributes of each design to a single metric that measures “goodness” for each of 3 stakeholders
  - Military User
  - Commercial User
  - Earth Science User
- Alternative Value Models
  - *Quality function deployment (QFD)*
  - *Analytic Hierarchy Process (AHP)*
  - *Cost-Benefit Analysis (CBA)*

Tradespace Exploration

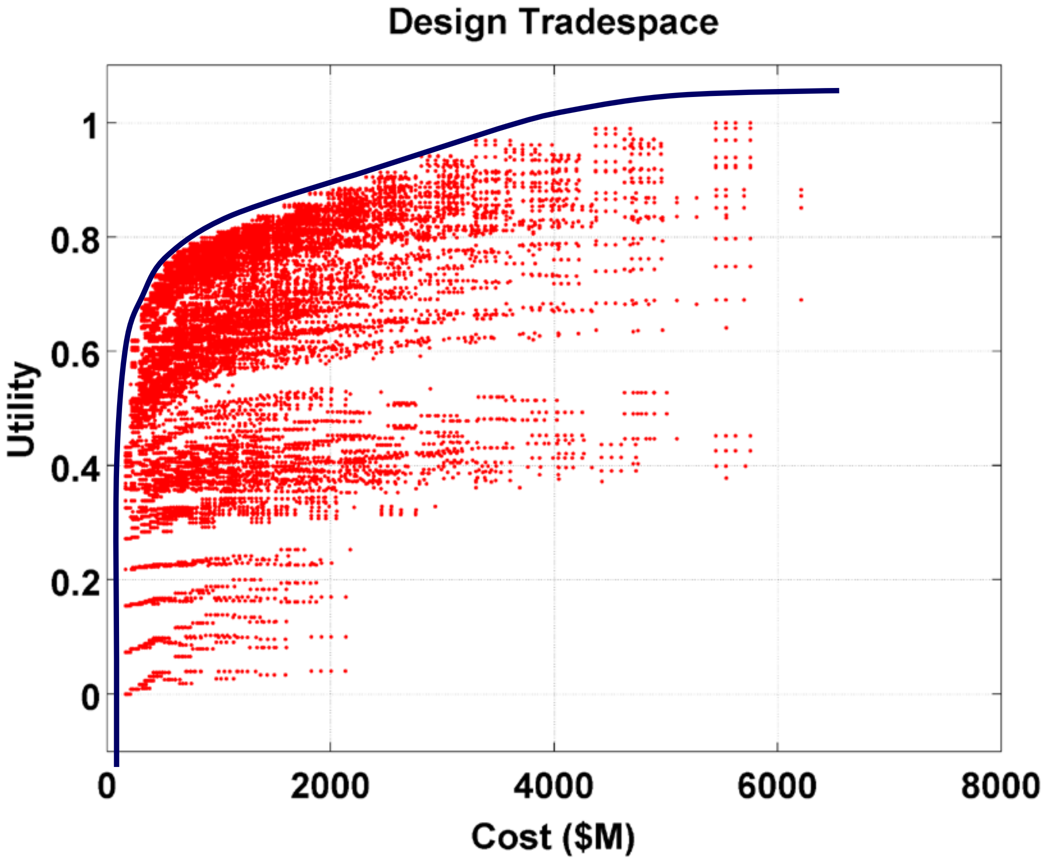
- A fractional factorial experiment (**14,400 designs**) can now be performed on the design variables to characterize the design tradespace
- Composite utility function, *U*, computed based on a weighted sum of the normalized performance metrics and evaluated against cost

Design Variables	Levels
Altitude (km)	250, 400, 600, 800
Inclination (deg)	0, 30, 60, 90, 100
# Orbital Planes	1, 2, 3, 4, 5, 6
# Satellites / plane	1, 2, 3, 4, 5, 6
Design Life (years)	1, 3, 5, 8
Aperture Diameter (m)	0.2, 0.5, 1.0, 1.5, 2.0



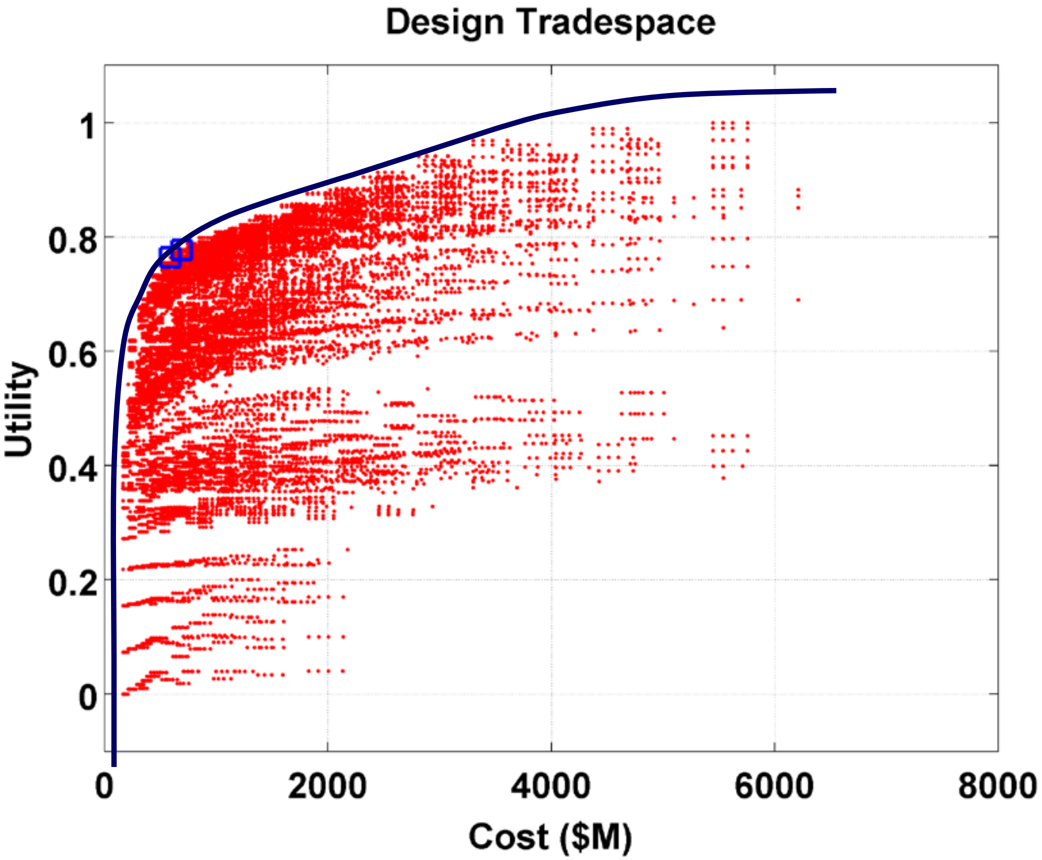
TSE Results

- A frontier of Pareto efficient solutions is apparent in a cost vs. utility scatter plot of available designs
- Traditionally, a designer would choose a design off the Pareto Front over alternative inferior designs



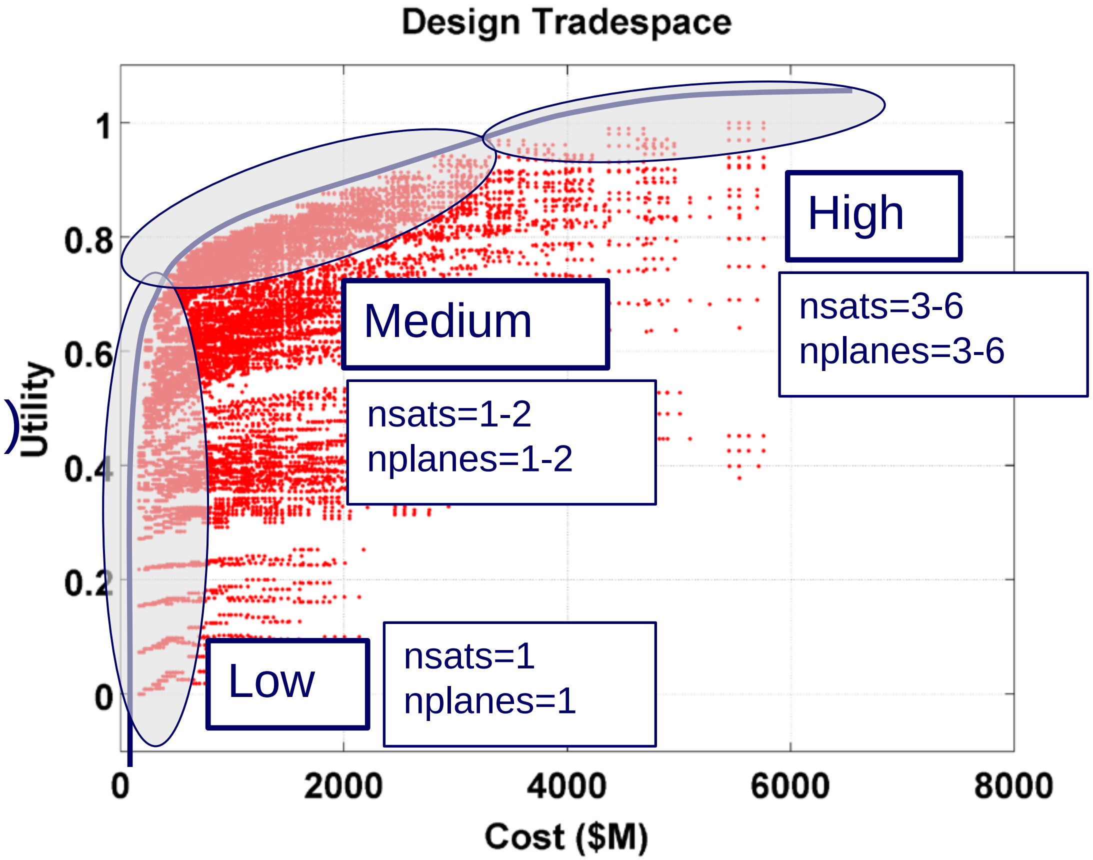
Multidisciplinary Optimization (MDO) Results

- A designer might also chose to use optimization techniques to find an ideal design
- Since this problem uses a mix of continuous and discrete variable, we can effectively apply heuristic optimizers such as:
  - Genetic Algorithms
  - Simulated Annealing
- Note that the optimizers choose designs on the Pareto Front as you would expect



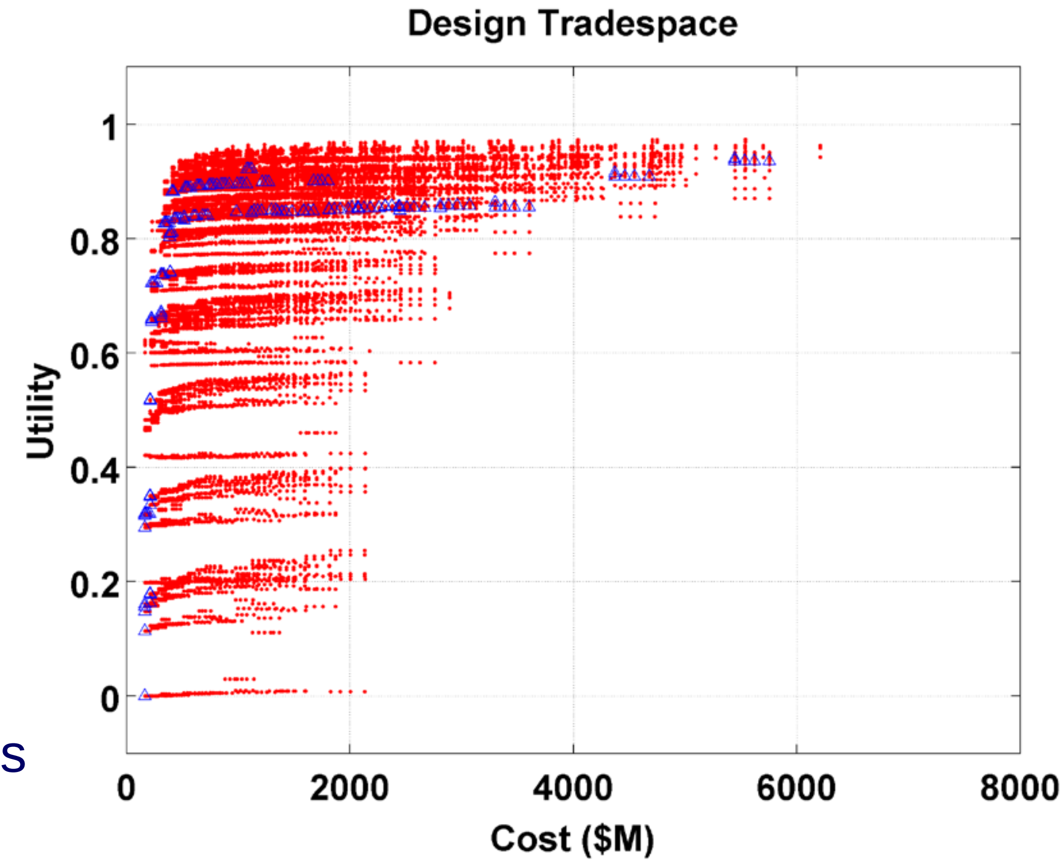
TSE Results

- Many of the designs along the Pareto front share common characteristics:
  - Altitude (800 km)
  - Global coverage (100%)
  - Polar orbits (90°-100°)
- In some areas along the Pareto front designs can be clustered into “families”



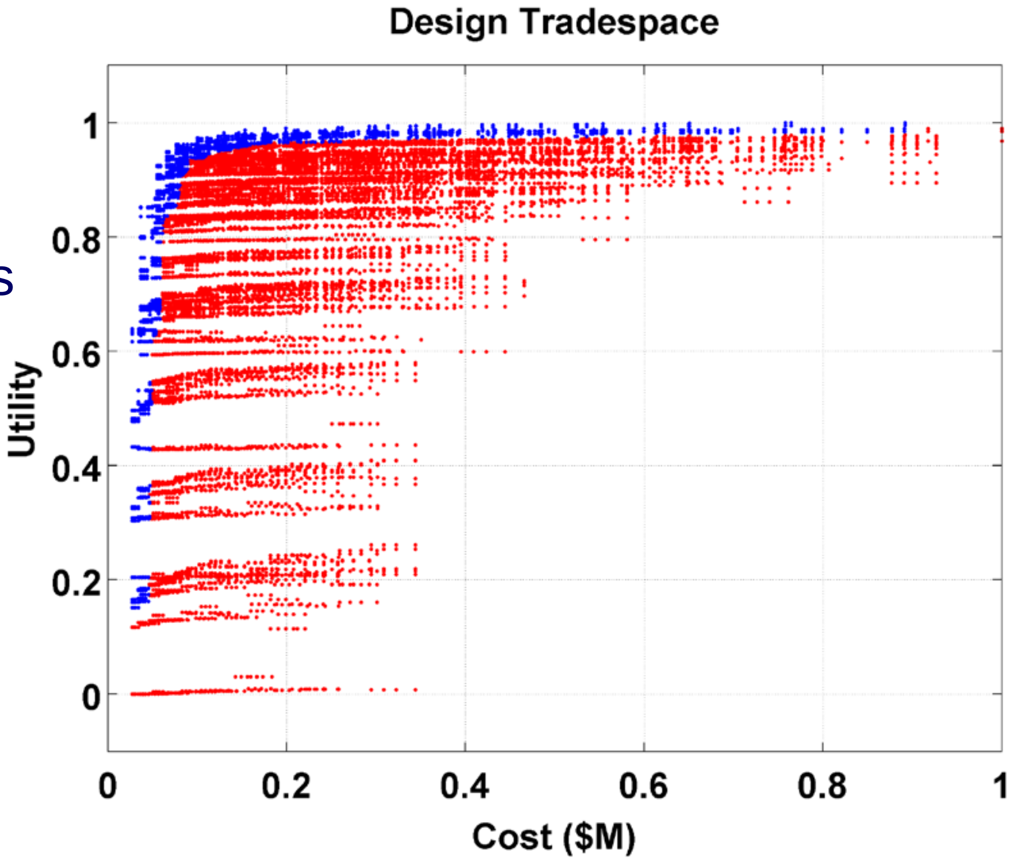
TSE Results

- But what if the context or needs change?
- The plot shows a shift in stakeholder needs that distort the previous tradespace
  - Mid-latitude coverage rather than global
  - Low revisit rate
- Points that were previously on the Pareto front (blue triangles) are not necessarily efficient designs anymore



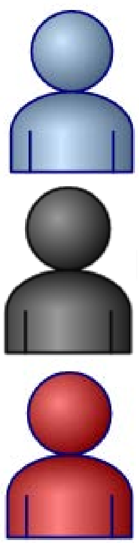
Fuzzy Pareto Number

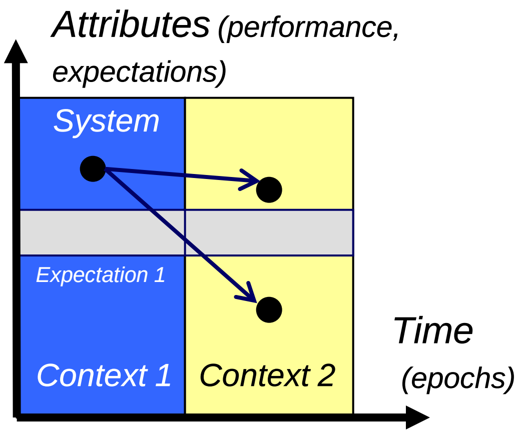
- If a design is required to be Pareto optimal across all contexts and needs it is unlikely that a compromise solution will exist
- By allowing additional points that are close to the Pareto front to be consider we can find a design that performs well enough across multiple epochs



Potential Perturbations (Epochs)

- Preference/Needs (Utility) function is different for each stakeholder
  - Military User (High Resolution, Low revisit time, Global coverage)
  - Commercial User (Medium Resolution, Medium revisit time, Mid-latitude coverage)
  - Earth Science User (Low Resolution, Low revisit time, Global coverage)
- 2 Possible future contexts also consider
  - EM event causes single event upset (SEU) to occur which leads to a loss of performance
  - No EM event occurs (e.g. status quo)
- **3 Needs** * **2 Contexts** = **6 Epochs**




Attributes (performance, expectations)

System

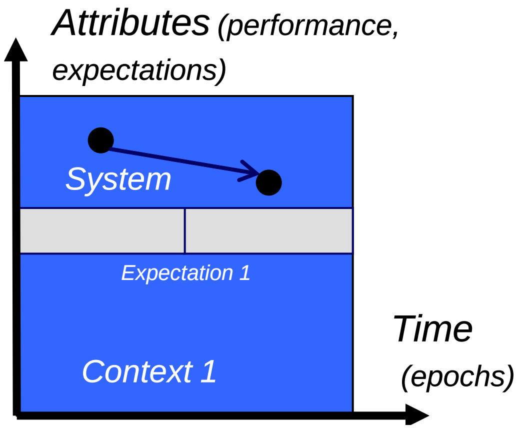
Expectation 1

Context 1

Context 2

Time (epochs)

EM event occurs


Attributes (performance, expectations)

System

Expectation 1

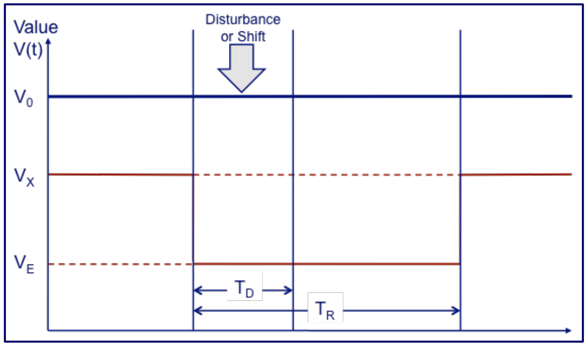
Context 1

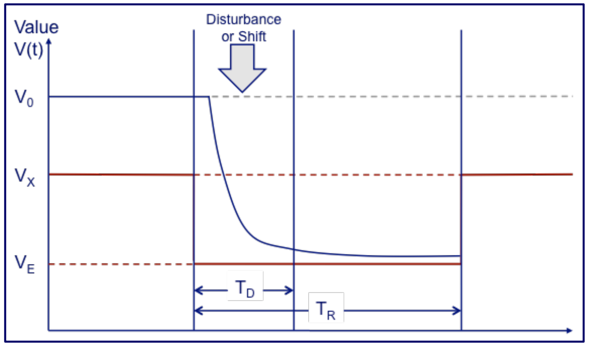
Time (epochs)

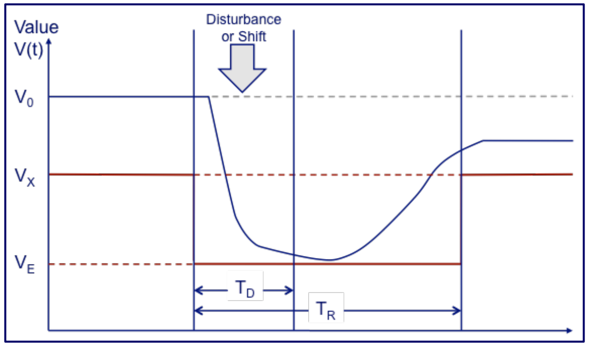
EM does not occur

Additional Design Options for Value Sustainment

Type I	Type II	Type III
<u>Mobility / Avoidance</u> - Prevent detection - Avoid EM	**<u>Hardness</u>** - Reduce impact of EM if it occurs	**<u>Replacement</u>** - Frequent replenishment of satellites
<u>Option</u>: Maneuvering Propellant - Additional mass which translates to added cost	**<u>Option</u>: Radiation Shielding** - Additional mass which translates to added cost	**<u>Option</u>: Lower Design Lifetime** - Launch replacements frequently to replenish capability



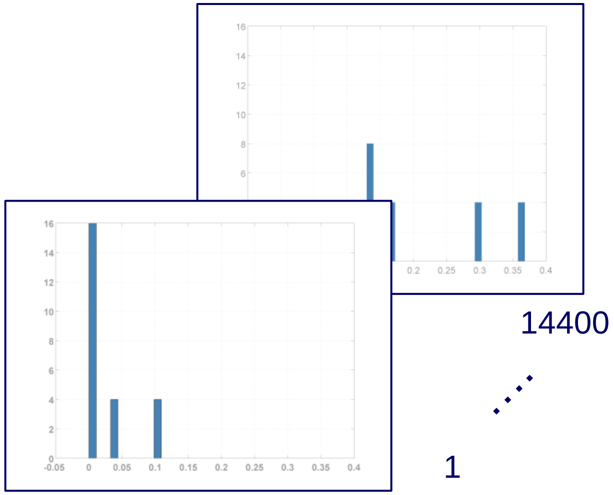




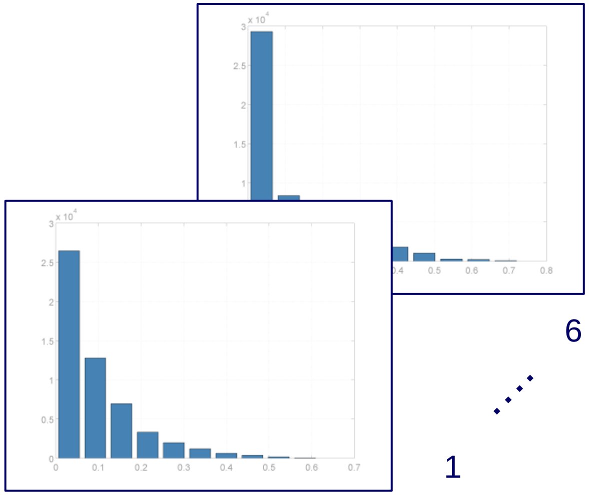
Multi Epoch Results

- Multi-Epoch results show a tension in preferred design alternatives between stakeholders, but 17 designs are Pareto efficient within an FPN of 10% and 4 designs are Pareto efficient within 5%
- Options 1, 3 and 4 allow at least one design to exist within the compromise design space

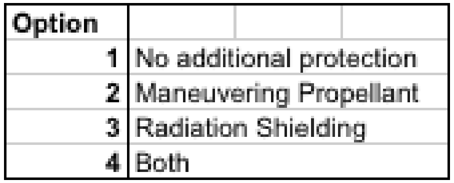
Design #	**4**	**9**	**4**	**9**	**28**	**3352**
Option	3	3	4	4	1	1
Inclination (deg)	90	90	90	90	60	90
Altitude (km)	250	400	250	400	400	400
Nsats	1	1	1	1	2	1
Nplanes	1	1	1	1	1	2
Design life (yrs)	1	1	1	1	1	1
Aperture (m)	0.2	0.2	0.2	0.2	0.2	0.5
Cost ($M)	$213	$208	$266	$259	$212	$310



Epochs across Designs



Designs across Epochs

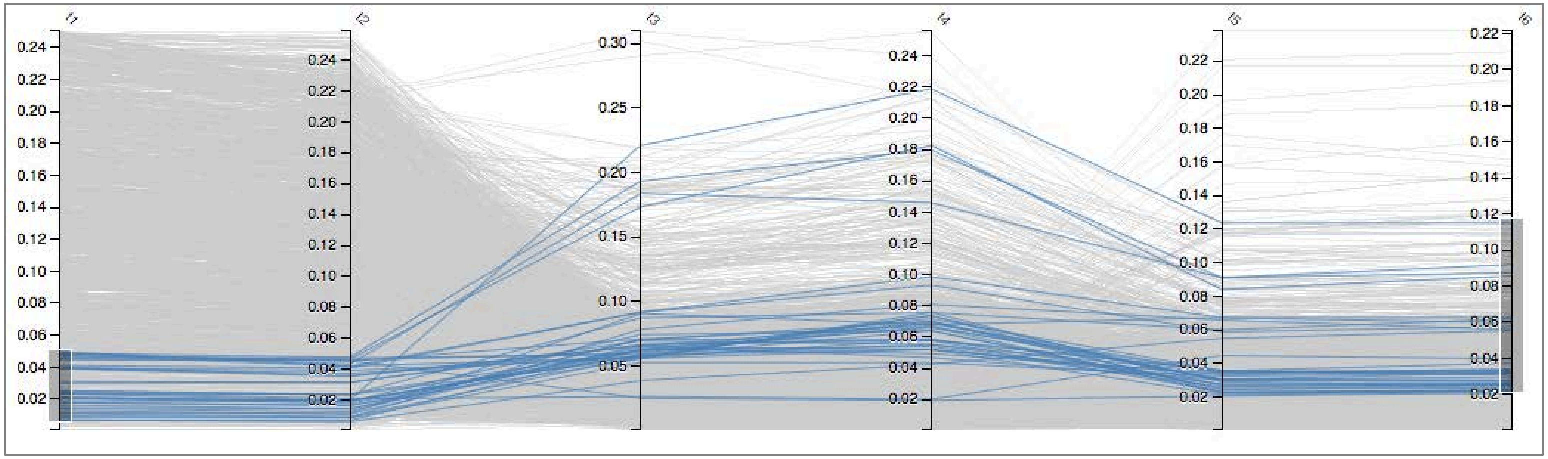


Option	
1	No additional protection
2	Maneuvering Propellant
3	Radiation Shielding
4	Both

14,400 Designs *
4 Design options *
<u>6 Epochs = </u>
345,600 Scenarios

Multi Era Results

- Eras take into account path dependencies between epochs
  - Designs that return to a “status quo” epoch after experiencing one that has an EM event do not recover all value
- Metrics to compare eras is a subject of ongoing research
- In general, current results show a bias in favor of protected designs because EM events are modeled as frequent events



Conclusions

- Designing resilient systems requires a shift in perspective vs. traditional tradespace exploration and multidisciplinary design optimization (MDO)
- Epoch-Era Analysis (EEA) generates a more complete picture of a system's value delivery across changes in stakeholder *needs*, operating *context* and the *system* itself
- Case study demonstrates how EEA can be used to find designs that sustain value over the system lifecycle

References

1. Ross, A., “Interactive Model-Centric Systems Engineering”. Briefing, 5th Annual SERC Sponsor Research Review, Washington, D.C., February 25, 2014.
2. Neches, R., “Engineered Resilient Systems S&T Priority Description and Roadmap”. NDIA 8th Annual Disruptive Technologies Conference, Nov 2011
3. Richards, M., Hastings, D., Rhodes, D., and Weigel, A., “Defining Survivability for Engineering Systems.” 5th Conference on Systems Engineering Research, Hoboken, NJ. March 2007.
4. Madni, A., “Affordable, Adaptable and Effective: The Case for Engineered Resilient Systems”, Engineering Resilient Systems Workshop, Pasadena, CA, August 2012.
5. Fitzgerald, M.E., Ross, A.M., and Rhodes, D.H., "A Method Using Epoch-Era Analysis to Identify Valuable Changeability in System Design," 9th Conference on Systems Engineering Research, Los Angeles, CA, April 2011.
6. Ross, A.M., and Rhodes, D.H., "Using Natural Value-centric Time Scales for Conceptualizing System Timelines through Epoch-Era Analysis," INCOSE International Symposium 2008, Utrecht, the Netherlands, June 2008.
7. Roberts, C.J., Richards, M.G., Ross, A.M., Rhodes, D.H., and Hastings, D.E., "Scenario Planning in Dynamic Multi-Attribute Tradespace Exploration," 3rd Annual IEEE Systems Conference, Vancouver, Canada, March 2009.