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

- 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”

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

Design$_i$ = \{X_1, X_2, X_3, ..., X_j\}

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”


• 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
  - 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)

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

Two aspects to an Epoch:
1. Needs (expectations)
2. Context (constraints including resources, technology, etc.)
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]
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

\[
\|J_i\| = \frac{J_i - J_{\text{nadir}}}{J_{\text{utopia}} - J_{\text{nadir}}}
\]

\[
Cost = \|J_1\|
\]

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

- 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)
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.
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 choose 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.
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 considered, 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
# Additional Design Options for Value Sustainment

<table>
<thead>
<tr>
<th>Type I</th>
<th>Type II</th>
<th>Type III</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mobility / Avoidance</strong></td>
<td><strong>Hardness</strong></td>
<td><strong>Replacement</strong></td>
</tr>
<tr>
<td>• Prevent detection</td>
<td>• Reduce impact of EM if it occurs</td>
<td>• Frequent replenishment of satellites</td>
</tr>
<tr>
<td>• Avoid EM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Option: Maneuvering Propellant**
- Additional mass which translates to added cost

**Option: Radiation Shielding**
- Additional mass which translates to added cost

**Option: Lower Design Lifetime**
- Launch replacements frequently to replenish capability

---

![Graphs showing value over time with disturbances and shifts for Type I, Type II, and Type III options.](image-url)
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.

<table>
<thead>
<tr>
<th>Design #</th>
<th>4</th>
<th>9</th>
<th>4</th>
<th>9</th>
<th>28</th>
<th>3352</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Inclination (deg)</td>
<td>90</td>
<td>90</td>
<td>90</td>
<td>90</td>
<td>60</td>
<td>90</td>
</tr>
<tr>
<td>Altitude (km)</td>
<td>250</td>
<td>400</td>
<td>250</td>
<td>400</td>
<td>400</td>
<td>400</td>
</tr>
<tr>
<td>Nsats</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Nplanes</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Design life (yrs)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Aperture (m)</td>
<td>0.2</td>
<td>0.2</td>
<td>0.2</td>
<td>0.2</td>
<td>0.2</td>
<td>0.5</td>
</tr>
<tr>
<td>Cost ($M)</td>
<td>$213</td>
<td>$208</td>
<td>$266</td>
<td>$259</td>
<td>$212</td>
<td>$310</td>
</tr>
</tbody>
</table>

14,400 Designs * 4 Design options * 6 Epochs = 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