Risk-based Resiliency Assessment Framework

Achieving Resilient U.S. Space Architectures

Andrew Long

October 2012

KTSi

Achieving Resilient U.S. Space Architectures

- "Resiliency" has become a key criterion in design of U.S. space systems
  - Assure military space-enabled functions
  - Prepare for operations within a degraded space environment
  - Account for hostile actions (man-made) and adverse conditions (natural)

US National Space Policy calls for increased "assurance and resilience of mission-essential functions… against disruption, degradation, and destruction, whether from environmental, mechanical, electronic, or hostile causes."

~ National Space Policy of the United States of America. 28 June 2010

US National Security Space Strategy calls for resilience as a key criterion in evaluating alternative [space] architectures.

US National Security Space Strategy. Jan 2011

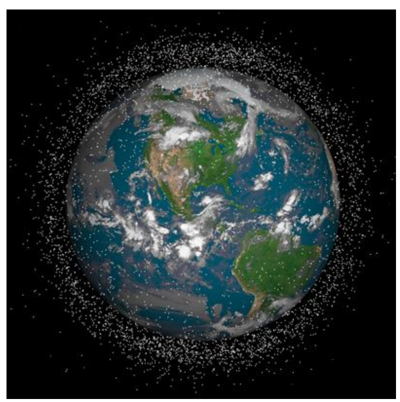
What is "Resiliency"

Resiliency is the ability of an architecture to support the functions necessary for mission success in spite of hostile action or adverse conditions.

An architecture is "more resilient" if it can provide these functions with higher probability, shorter periods of reduced capability, and across a wider range of scenarios, conditions and threats

- OSD Policy Approved Definition, 2011

Threat Continuum



Natural | Adverse | Hostile actions (man-made)

How does one measure and design for "Resiliency"?

Resiliency Evaluation

US DoD and DNI provide the following evaluation criteria as a common means to assess resilience for any given functional architecture

"Resilience of Space Capabilities". US Department of Defense and Office of the Director for National Intelligence, National Security Space Strategy. Accessed 11 March 2012.

- Anticipated level of adversity
  - Disturbance (Natural, Man-made, Hostile, etc)
  - Disturbance Awareness (Ability to identify potential disturbances)
- Functional **capability goals** necessary to support the mission (Mission essential Function, Capability Need, Measures of Performance, etc.)
- The **risk** that these goals may not be met at a given level of adversity
- The **severity** of the functional shortfall to the mission
- The **time** which the shortfall can be tolerated by the mission

Challenge: Context - Dependent (Mission, Scenario, etc.)

Resiliency is a multi-context (dynamic) problem!

Survivability (Static Context)

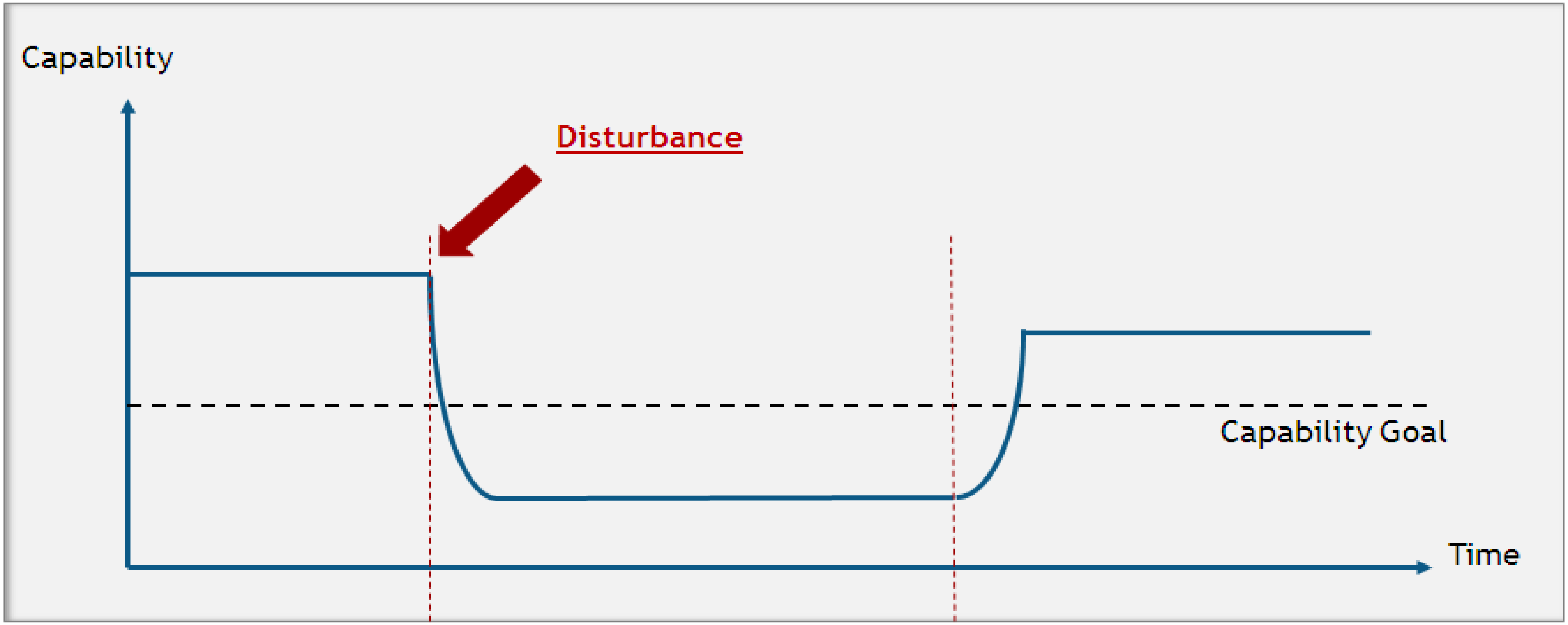
Survivability Elements

- **Awareness:** Ability to detect, characterize, and/or attribute a given threat.
- **Susceptibility*,+:** The degree to which a weapon system is open to effective attack due to one or more inherent weakness.
- **Vulnerability*,+:** The characteristic of a system that causes it to suffer a definite degradation as a result of having been subjected to a certain level of effects in an unnatural hostile environment.
- **Recovery*:** Following combat damage, the ability to take emergency action to prevent loss of the system, to reduce personnel casualties, or to regain weapon system combat mission capabilities.

** Department of Defense (DoD) Regulation 5000.2-R (2002)*

+ DAU Glossary of Defense Acquisitions Acronyms & Terms, 13th ed.

Survivability: Visual Pictorial

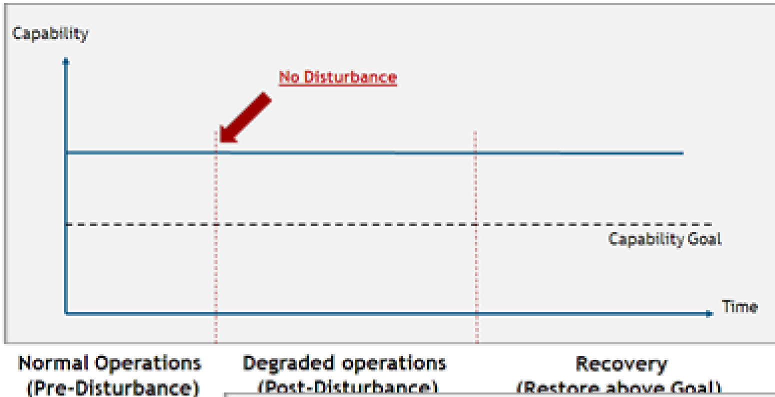


Normal Operations (Pre-Disturbance)

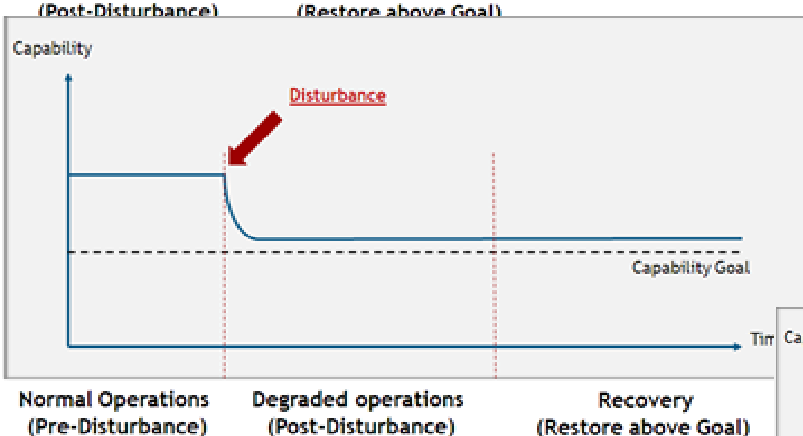
Degraded operations (Post-Disturbance)

Recovery (Restore above threshold)

Disturbance Mitigation Strategies

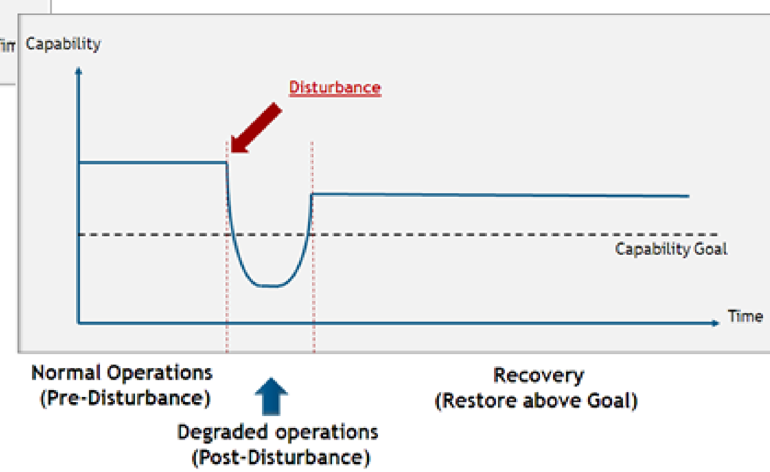


Notional Protected Architecture
(Low Susceptibility)



Notional Endurable Architecture
(Low Vulnerability)

Notional rapidly recoverable architecture
(Rapid Recovery)



Survivability: Design Principles

Susceptibility Reduction	
Prevention	Suppression of a future or potential future disturbance
Mobility	Relocation to avoid detection by an external agent
Concealment	Reduction of the visibility of a system from an external agent
Deterrence	Dissuasion of a rational external agent from committing a disturbance
Preemption	Suppression of an imminent disturbance
Avoidance	Maneuverability away from an ongoing disturbance

Vulnerability Reduction	
Hardness	Resistance of a system to deformation
Heterogeneity	Variation in system elements to mitigate homogeneous disturbances
Distribution	Separation of critical system elements to mitigate local disturbances
Fail-safe	Prevention or delay of degradation via characteristics of incipient failure

Impact Reduction	
Redundancy	Duplication of critical system functions
Margin	Allowance of extra capability for maintaining value despite impact
Failure mode	Reduction elimination of system hazards through intrinsic design: substitution, simplification, etc.
Evolution	Alteration of system elements to reduce disturbance effectiveness
Containment	Isolation or minimization of the propagation of failure

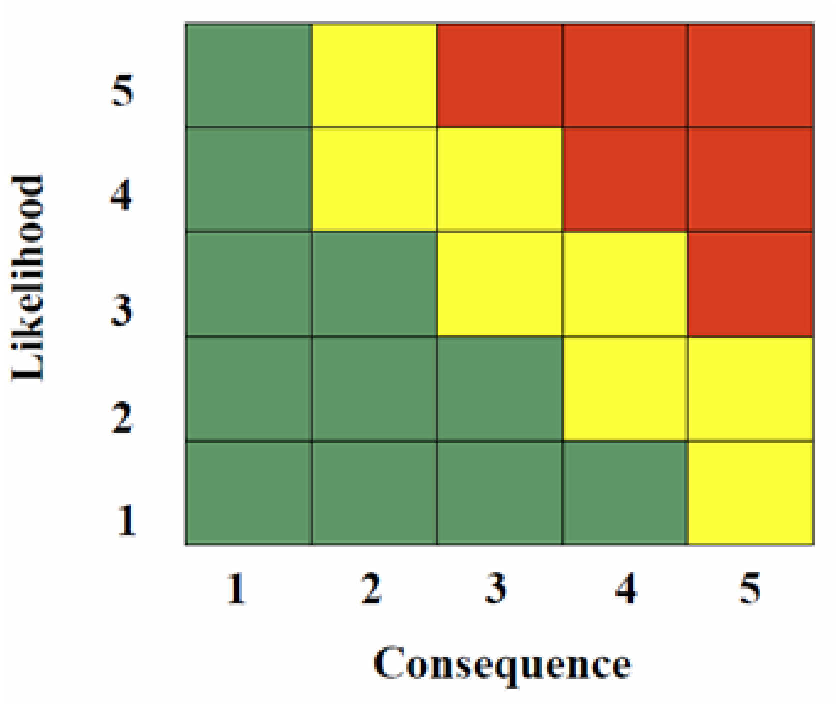
Recovery Enhancement	
Replacement	Substitution of system elements to recovery value
Repair	Restoration of system to recover value

Richards, M.G., Hastings, D.E., Rhodes, D.H., and Weigel, A.L., "Defining Survivability for Engineering Systems," 5th Conference on Systems Engineering Research, Hoboken, NJ, March 2007

DoD Risk Assessment

Three components are utilized in evaluating risk:

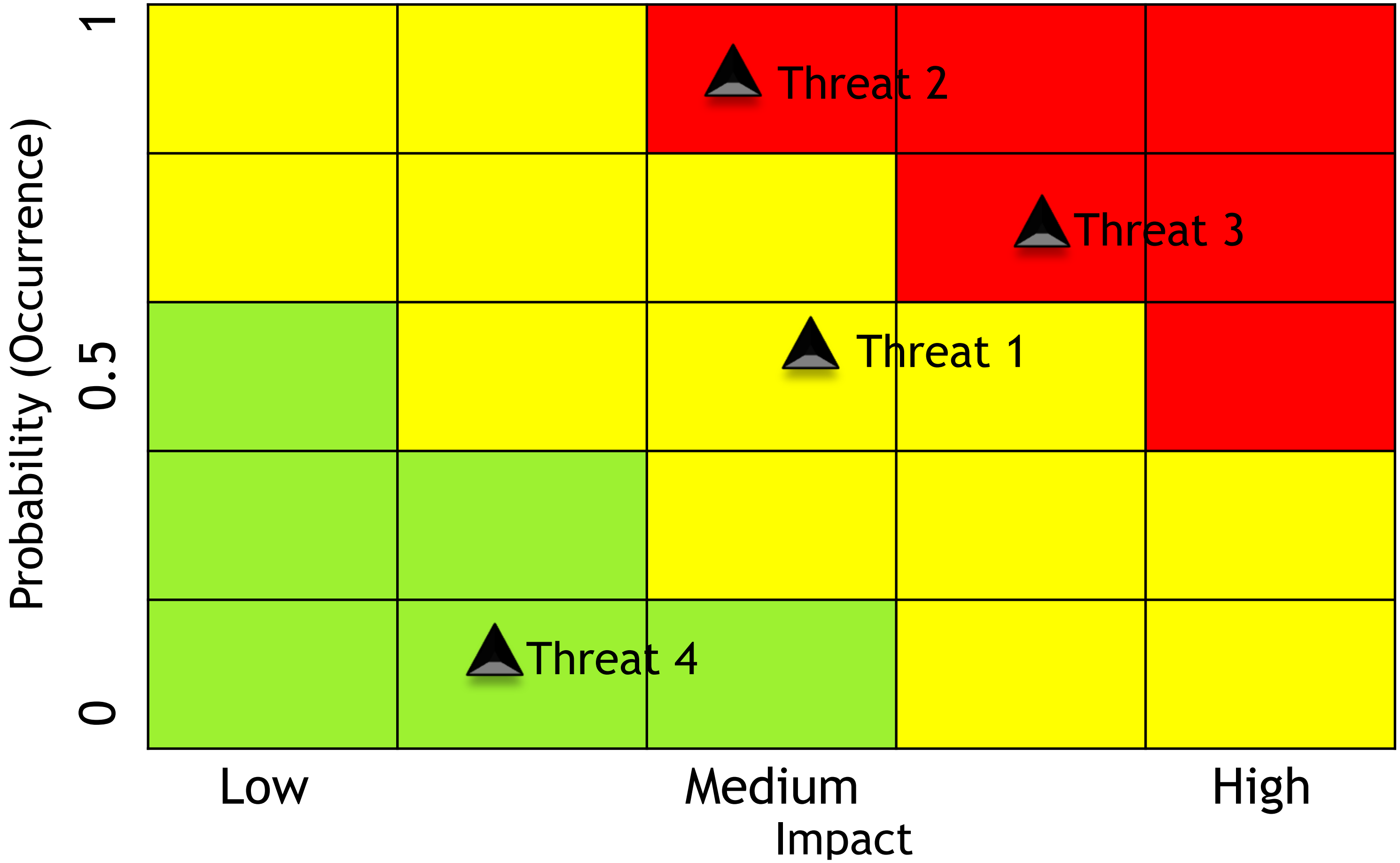
1. Potential disturbance
2. Probability (or likelihood) of the future
   disturbance occurring
3. Consequence (or effect)



Risk Reporting Matrix

RISK MANAGEMENT GUIDE FOR DOD ACQUISITION, Sixth Edition. August, 2006.
US Department of Defense, Acquisition, Technology, and Logistics (OSD/AT&L)

Survivability Assessment of Risk Posture

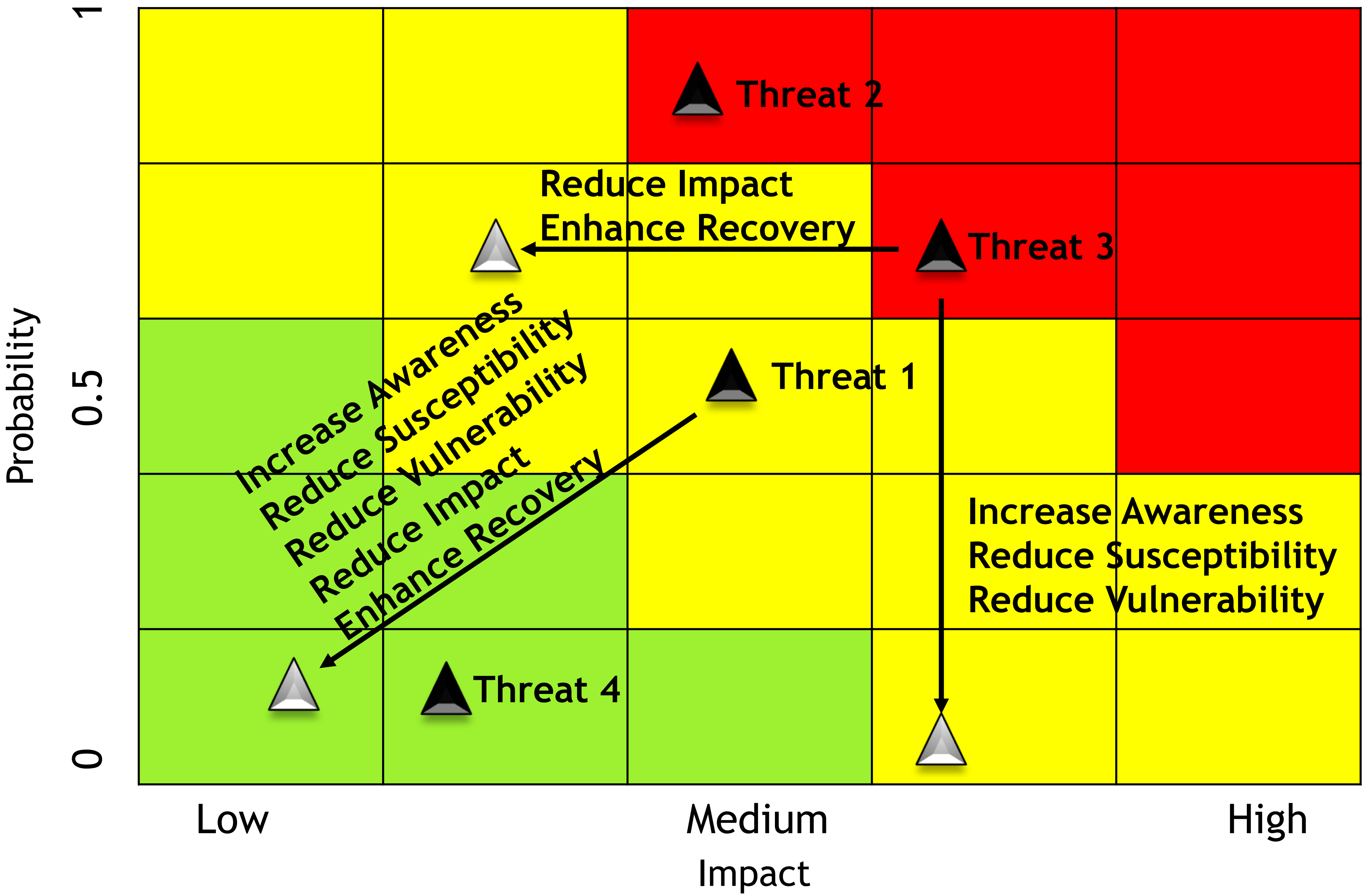


$$p(\text{occur}) = p(\text{Threat}) * intent * \left[\left(p(\text{A})p(S_1)p(V_1)\right) + \left(1 - P(\text{A})\right)p(S_2)p(V_2)\right]$$

$$Impact = \sum W_i D_i,$$

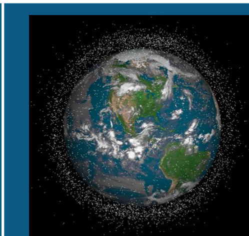
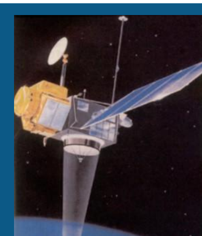
where D_i = f(Capability Loss, Outage Duration, Recovery Cost, etc.) & W_i = Weighting

Identify Risk Mitigation Approaches



Resiliency Assessment

Contexts

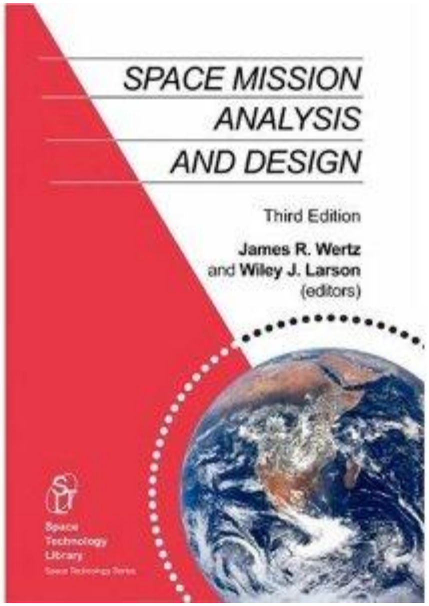
Mitigation Options					Resiliency Assessment	
Baseline	Green	Yellow	Red	Red	Red	$
Increase Awareness	Green	Yellow	Yellow	Red	Yellow	$$
Reduce Susceptibility	Green	Green	Yellow	Red	Yellow	$$$
Reduce Vulnerability	Green	Green	Green	Red	Yellow	$$$$
Reduce Impact	Green	Green	Green	Red	Yellow	$$$$$
Enhance Recovery	Green	Green	Green	Green	Green	^{10}

Questions

Example

FireSat

FireSat Overview



Design Tradespace

Design Variable	Sample
Aperture	0.2 - 0.9m
Altitude	400 – 1000km
Inclination	30 - 75 deg
Design Life	4-10 yrs
# Sats	1-3

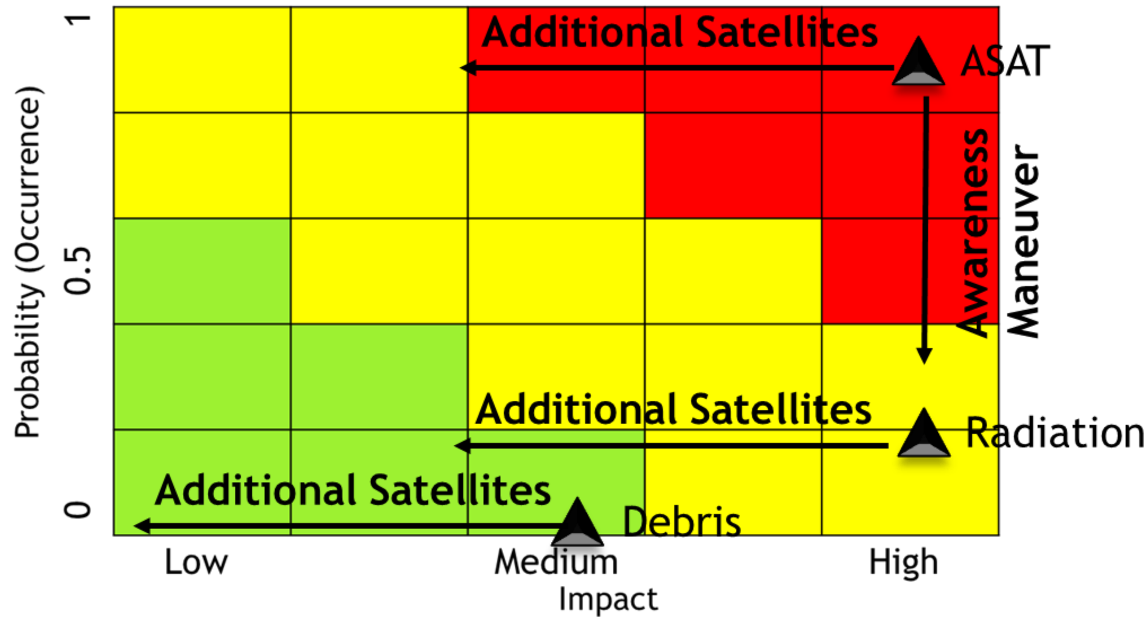
Notional “Threat” Assessment

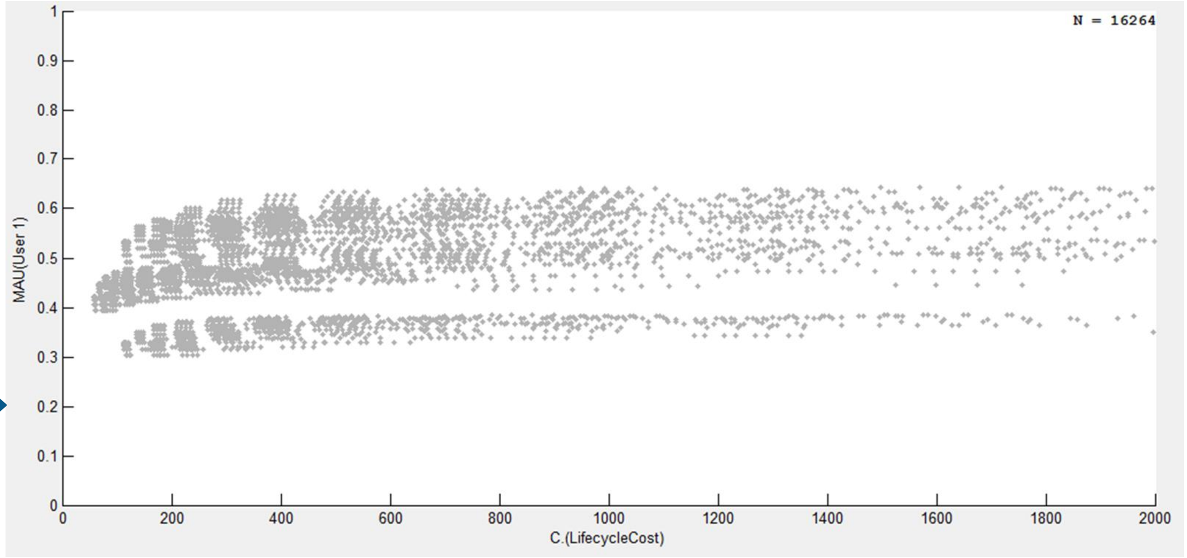
Threat	P(Threat)	Intent	P(A)	$P(S_1)$	$P(V_1)$	$P(S_2)$	$P(V_2)$	P(Occur)
Radiation	0.2	1	1	1	1	1	1	0.2
Debris	0.1	1	0.9	0.2	1	1	1	0.028
ASAT	1	1	0	0.9	1	1	1	0.95
ASAT	1	1	0	0.9	1	1	1	0.95

Resiliency Evaluation

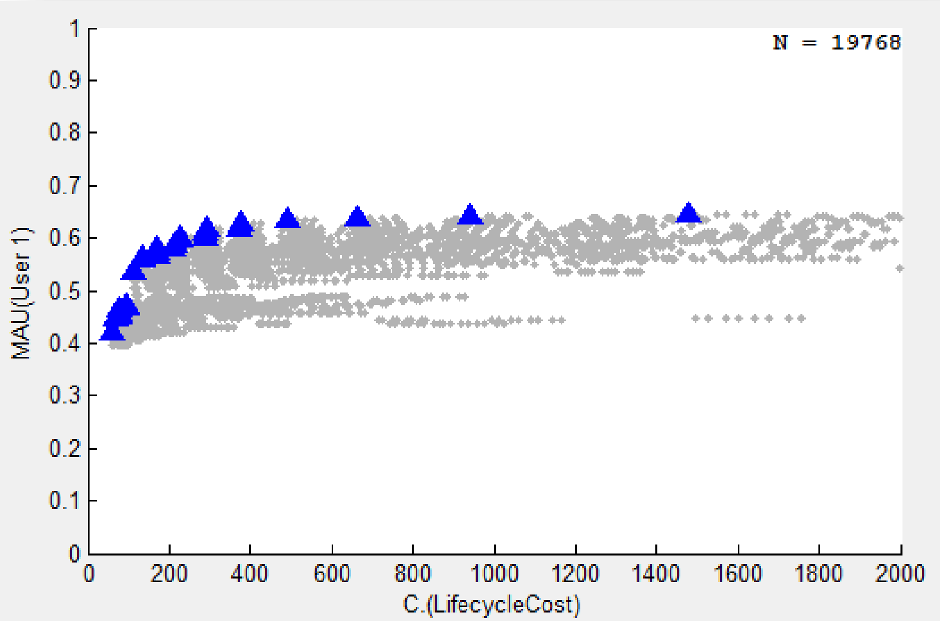
Modified Design Tradespace

Design Variable	Sample
Aperture	0.2 - 0.9m
Altitude	400 – 1000km
Inclination	30 - 75 deg
Design Life	4-10 yrs
# Sats	1-3
Hardening	Yes / No
Maneuvers	Yes / No
Awareness Sensors	Yes / No





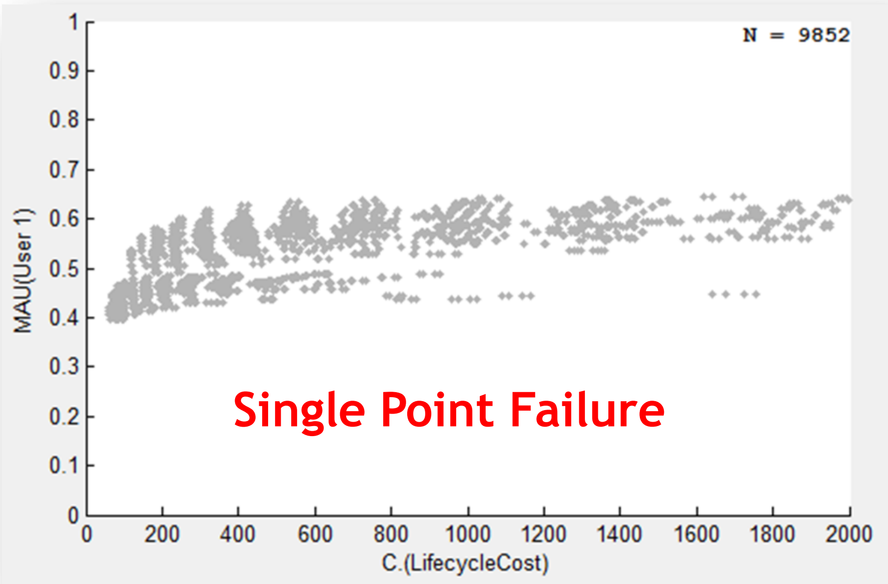
"Best Design" - Benign Environment

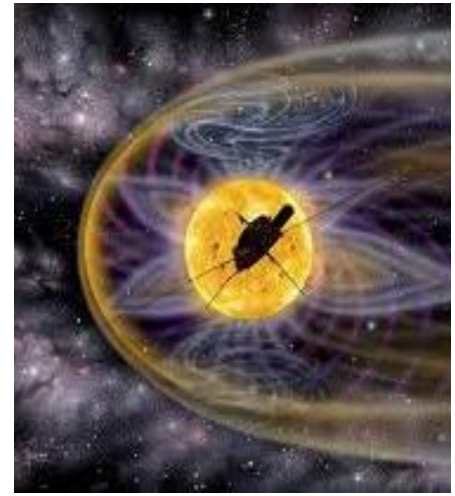


No Survivability Measures
(e.g Awareness, Maneuver, Hardening, etc.)

Aperture	0.2m	0.3m	0.4m	0.5m	0.6m	0.7m	0.8m	0.9m
Altitude	1000km	900-1000km	700-1000km	900-1000km	1000km	1000km	1000km	1000km
Inclination	75	75	75	75	75	75	75	75
Design Life	10	10	10	10	10	10	10	10
# Sats	1-2	1-3	1-3	1-3	1	1	1	1
Lifecycle Cost	$57-111M	$66-227M	$77-290M	$92-376M	$497M	$663M	$942M	$1,478M

"Best Design" in non-benign Environment

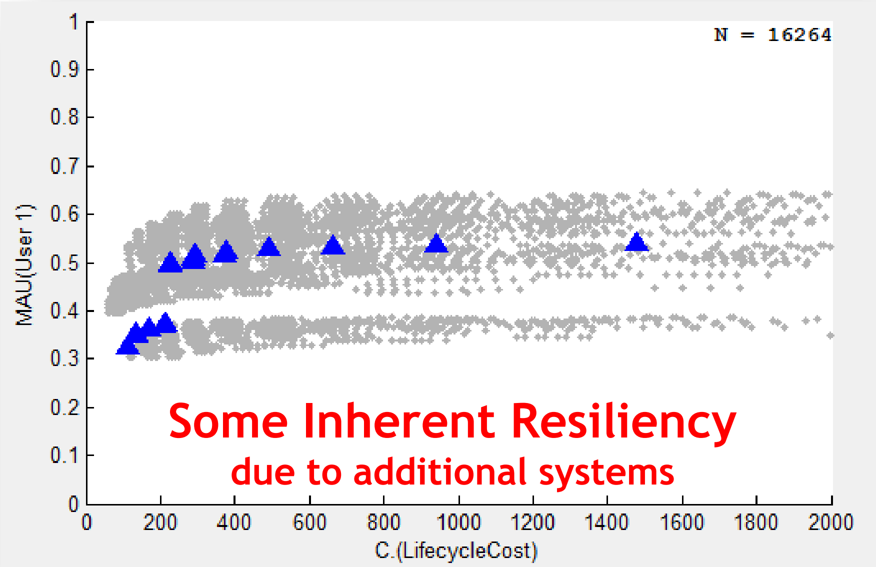




No Survivability Measures
(e.g Awareness, Maneuver, Hardening, etc.)

Aperture	0.2m	0.3m	0.4m	0.5m	0.6m	0.7m	0.8m	0.9m
Altitude	1000km	900-1000km	700-1000km	900-1000km	1000km	1000km	1000km	1000km
Inclination	75	75	75	75	75	75	75	75
Design Life	10	10	10	10	10	10	10	10
# Sats	1-2	1-3	1-3	1-3	1	1	1	1
Lifecycle Cost	$57-111M	$66-227M	$77-290M	$92-376M	$497M	$663M	$942M	$1,478M

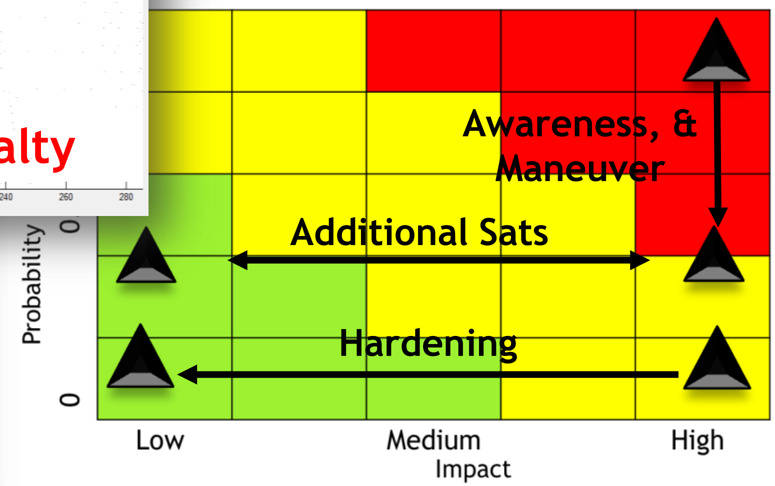
"Best Design" in Contested Environment



No Survivability Measures
(e.g Awareness, Maneuver, Hardening, etc.)

Aperture	0.2m	0.3m	0.4m	0.5m	0.6m	0.7m	0.8m	0.9m
Altitude	1000km	900-1000km	700-1000km	900-1000km	1000km	1000km	1000km	1000km
Inclination	75	75	75	75	75	75	75	75
Design Life	10	10	10	10	10	10	10	10
# Sats	2	2-3	2-3	2-3	1	1	1	1
Lifecycle Cost	$57-111M	$66-227M	$77-290M	$92-376M	$497M	$663M	$942M	$1,478M

"Best Resilient" Systems



Aperture	0.2m	0.3m	0.4m	0.5m	0.6m	0.7m	0.8m	0.9m
Altitude	1000km	900-1000km	700-1000km	900-1000km	1000km	1000km	1000km	1000km
Inclination	75	75	75	75	75	75	75	75
Design Life	10	10	10	10	10	10	10	10
# Sats	1-2	1-3	1-3	1-3	1	1	1	1
Lifecycle Cost	$57-111M	$66-227M	$77-290M	$92-376M	$497M	$663M	$942M	$1,478M
	$60-120M	$70-251M	$83-325M	$109-420M	$559M	$758M	$1,084M	$1,718M