THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

NDIA
National Defense Industrial Association

Resilience Engineering Heuristic Design Principles

NDIA 19th Annual Systems Engineering Conference
October 24-27, 2016

Kenneth V. Stavish

in partial fulfillment of the requirements for a Doctor of Philosophy degree
The George Washington University

Additional Authors: Dr. Timothy Blackburn
Dr. Andreas Garstenauer

Purpose of Resilience Eng. Design Principles

Proceeding Overview

- Relationship between two tracks of **Resilience Engineering**:
  i. Techniques to assess and measure resilience
  ii. Resilience engineering design principles grounded in heuristics [1,2]

Which design principles have been the most effective, and for which aspects of resilience?

- Example: Applying resilient design principles to Inertial Navigation Systems

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Purpose of Resilience Eng. Design Principles

Architecting and Design of Resilient Systems

Current State [3]

Systems are designed with fault detection, isolation, and recovery in mind. Fault detection is based on probabilistic and empirical characterizations of off-nominal behavior.

Vision for the Future [3]

Architecting will incorporate design approaches for systems to perform their intended functions in the face of changing circumstances or invalid assumptions.

Demonstrated Assessment Techniques

- Infrastructure systems [4,5]
- Organizational systems [8]
- Biological ecosystems
- Engineered products [6]

Design Principles

- Grounded in experience and knowledge [2]
- Missing validation and relationship models to assessment techniques, particularly for assessing engineered systems.

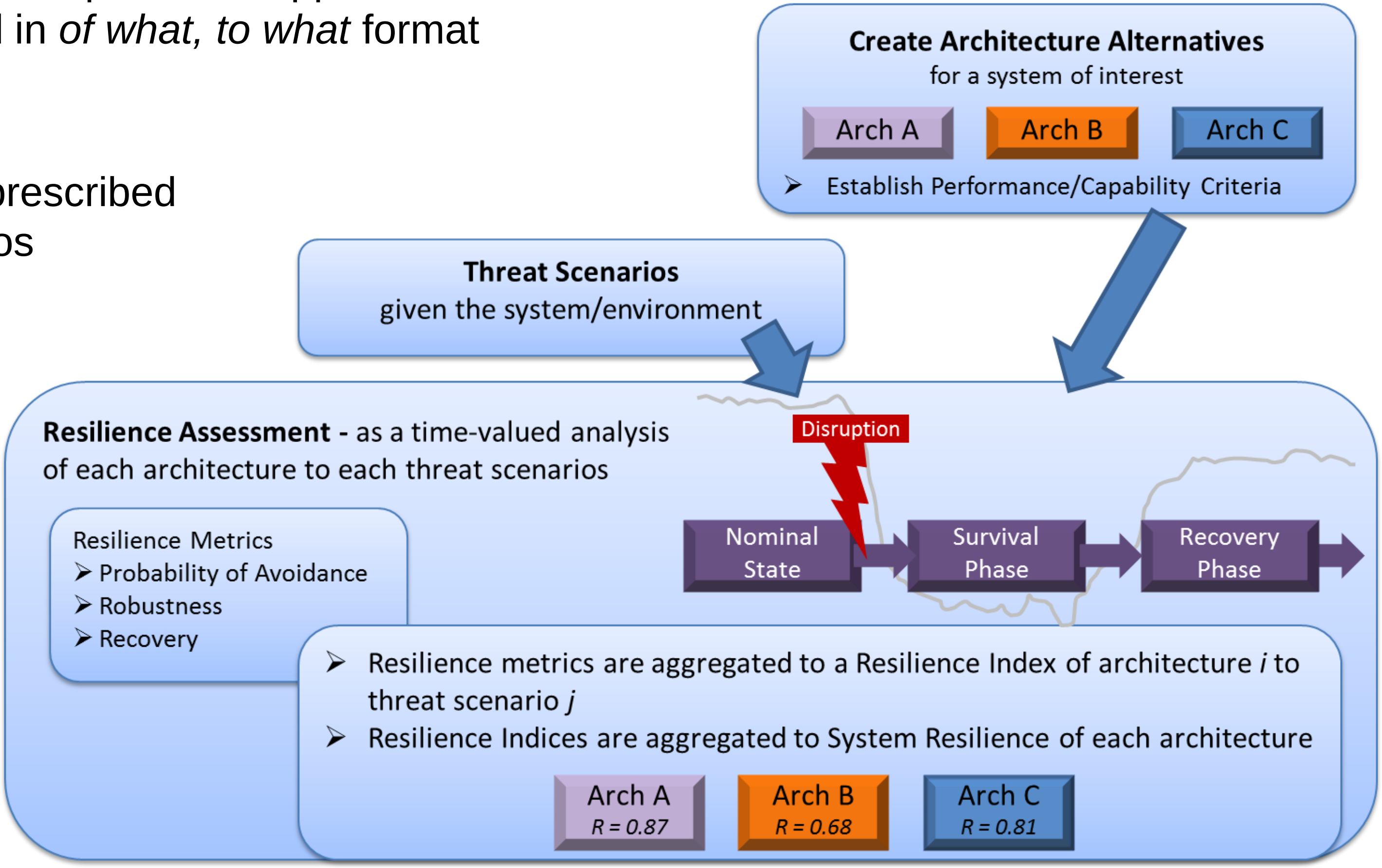
Resilience Assessment Techniques

Resilience Assessment Techniques
are the current focus of an emerging resilience engineering discipline [4,5,6]

Demonstrated Approaches
- Developed and tested for particular applications
- Resilience expressed in *of what, to what* format

Threat Scenarios
- Disruption modeling prescribed through fixed scenarios

Measuring Resilience
- Probabilistic models
- Temporal analyses
- Time-valued metrics



Threats and Disruptions

Resilience is measured against one or more threats

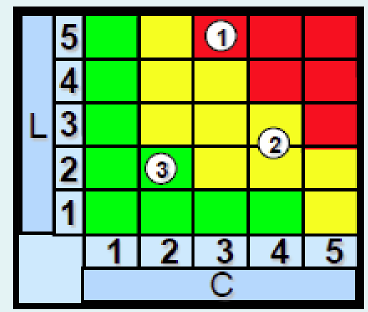
'the resilience of system X to threat Y'

Threat Considerations

- Any condition that results in loss of capability
- Systematic and/or external inputs
- Man-made or natural threats
- Singular threats against one system element or simultaneous threats against multiple elements
- Resonance: large consequences can arise from small variations in performance and conditions

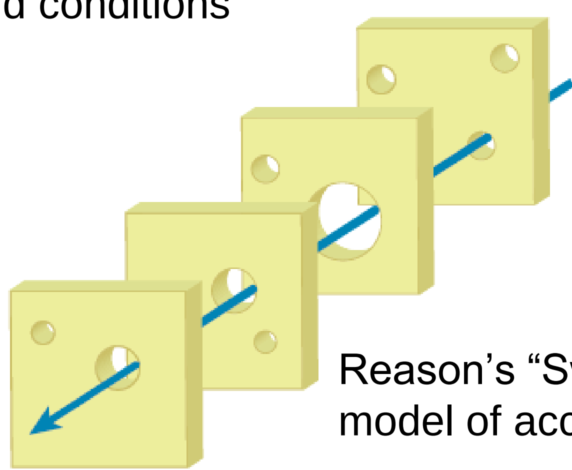
Disruption Analysis

- Identify disruptions, low likelihood high-impact, known and unknown (unexpected) disruptions



Define Disruption Scenarios

- Scenarios of single or multiple, coordinated disruptions.



Reason's "Swiss cheese" model of accident causation [9]

Mechanisms of Resilience

	Description	Anecdotal Description
Recovery	Capacity to perform system functions following a disturbance.	Autonomous vehicle is able to get upright after being tipped over by strong winds.
Robustness	Capacity to perform system functions during a disturbance.	Autonomous vehicle does not tip over in the face of strong winds.
Avoidance	Capacity of the system to change functional behaviors or system configurations according to new or changing conditions.	Autonomous vehicle reconfigures its waypoints in the face of changing wind patterns.

Calculation of Resilience

$$R_{i,j} = R_{AV} + (1 - R_{AV})R_{RO} + (1 - R_{AV})(1 - R_{RO})R_{RV}$$

- $R_{i,j}$: Resilience Index
- R_{AV}: Prob. Of Avoidance
- R_{RO}: Robustness Metric
- R_{RV}: Recovery Metric

Avoidance: R_{AV} estimates the probability of fully avoiding a disruption

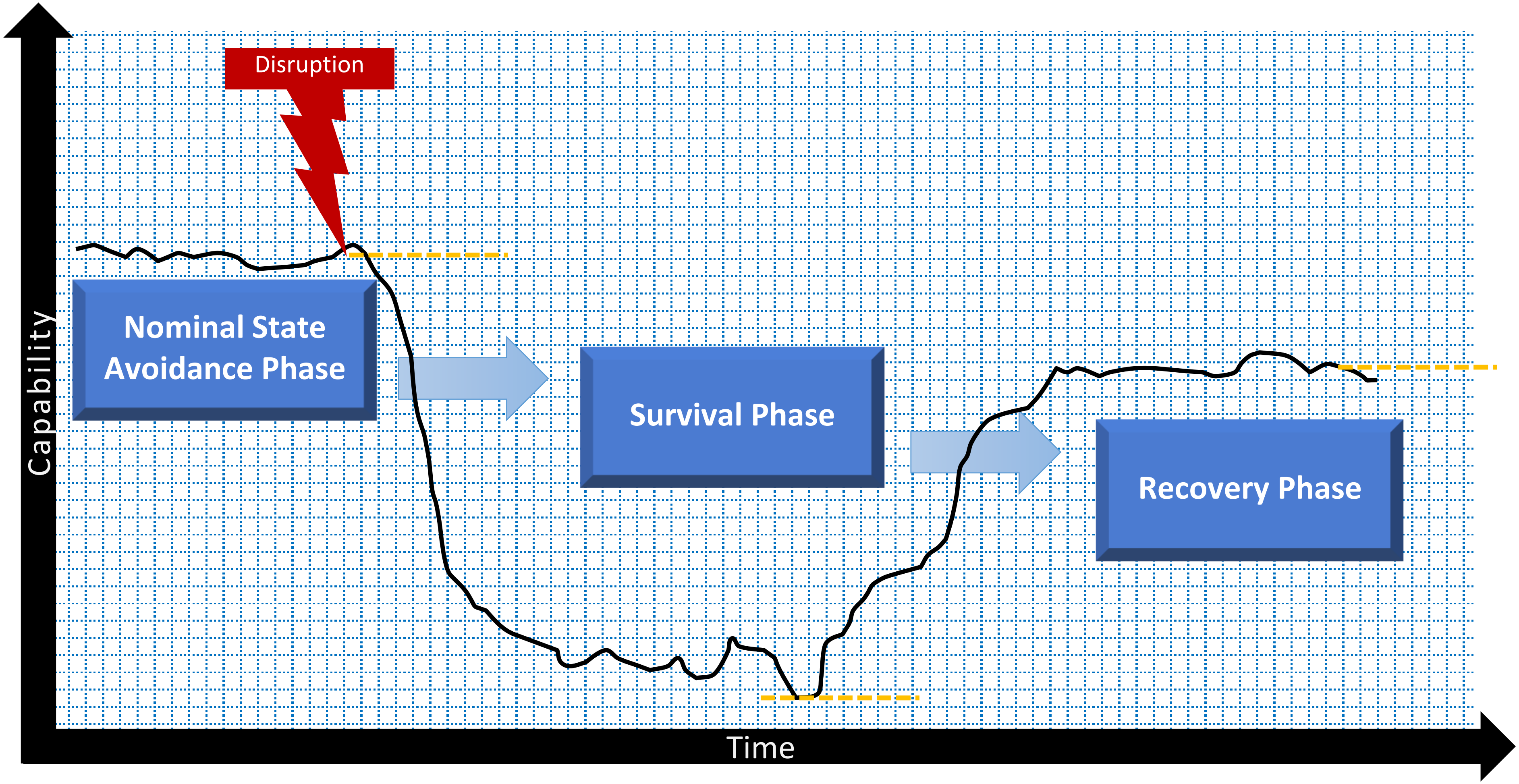
Robustness: R_{RO} is the minimum capacity retained following a disruption

Recovery: R_{RV} is a how much and how quickly lost capability can be recovered following the presence of a disruption

Resilience Index: $R_{i,j}$ is the resilience index of architecture *i* to disruption *j*

- This calculation for measuring resilience was adapted from (Burch, 2013) [6].
- The calculation captures that there are multiple methods of achieving resilience, and each metric is weighted equally.

Temporal Phases of Resilience



THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Resilience Engineering Design Principles

Design Principle	Heuristic: "rule of thumb" for systems engineering [1,2,8]
Functional Redundancy	Design alternative methods to perform particular functions that do not rely on the same physical components
Physical Redundancy	Include redundant hardware, including computer processors
Reorganization	Design an ability for the system to restructure itself in response to an external change
Absorption	Include adequate margin to withstand threats
Human-in-the-Loop	Include humans interaction where rapid cognition is needed
Loose Coupling	Limit the ability of failures to propagate from one component to the next in a system of many components
Complexity Avoidance	Avoid complexity added by poor human design practice
Localized Capacity	Design functionality through various nodes of the system so that if a single node is damaged or destroyed, the remaining nodes will continue to function.
Drift correction	Monitor and correct if the system is drifting towards boundaries of capability
Neutral state	Prevent further damage from occurring when hit with an unknown perturbation until the problem can be diagnosed
Reparability	Design the ability to repair system elements
Inter-node Interaction	Design communication, cooperating, and collaborating between system elements
Reduce Hidden Interactions	Potentially harmful interactions between nodes of the system should be reduced
Layered Defense	Use two or more independent principles that address a single element of system vulnerability

Resilience Attributes

Capacity Attribute

This attribute is the ability of the system to survive a threat

Absorption

Functional Redundancy

Physical Redundancy

Layered Defense

Flexibility Attribute

This attribute is the ability of the system to adapt to a threat

Reorganization

Human-in-the-loo

Complexity Avoidance

Reparability

Loose Coupling

Tolerance Attribute

This attribute is the ability of the system to degrade gracefully in the face of a threat

Localized Capacity

Drift Correction

Neutral State

Cohesion Attribute

This attribute is the ability of the system to act as a unified whole in the face of a threat

Inter-node Interactions

Reduce Hidden Interactions

Heuristics Analysis

Data Mining System

- Method to quantify past performance of architecting with resilience design principles

Criterion

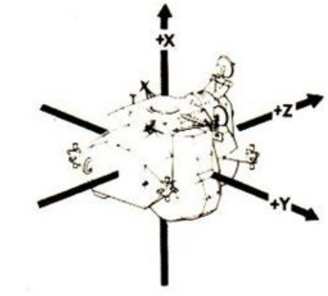
- ➢ Evidenced in published requirements, patents, and design documentation
- ➢ Does requirement *X* explicitly show that architecting system element *Y* considered resilience engineering design principle *Z*?

Measure	Descriptor
0	None
1	Marginal
2	Nominal / Some
3	Wide
4	Extensive

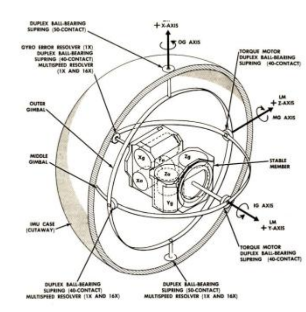
Example: Inertial Navigation Systems

Inertial Navigation Systems
System components
Aligned to Heuristic Analysis

		Absorption	Physical Redundancy	Functional Redundancy	Layered Defense	Reorganization	Human in the loop	Reduce Complexity	Reparability	Loose Coupling	Localized Capacity	Drift Correction	Neutral State	Inter-node interactions	Reduce hidden interactions
GPS Coupling	Loose Coupling	4	0	2	0	0	0	0	2	1	0	4	2	1	1
	Tight Coupling	2	0	3	4	2	0	0	1	0	0	4	0	3	2
	Deeply Integrated	3	0	3	4	4	3	4	2	0	3	3	1	0	3
Augmentation Sensors	Wide Band RF	2	1	2	0	0	2	0	0	1	1	2	2	2	0
	Magnetometer	0	0	4	3	2	0	0	0	2	4	0	1	1	0
	Velocity Meter	1	2	0	3	3	1	4	0	0	4	1	1	4	0
	Baroaltitude	0	0	4	0	4	0	2	0	3	0	1	0	1	0
Gyro	Ring Laser Gyros (RLG)	2	0	2	1	0	0	3	2	1	2	0	3	0	0
	Fiber Optic Gyros (FOG)	2	3	4	0	4	0	4	0	2	0	0	4	2	0
	MEMS	0	0	0	1	1	0	0	0	0	4	0	0	1	0
Platform	Gimballed	1	4	0	0	4	4	1	0	1	0	0	1	1	1
	Strapdown	0	2	0	2	0	2	0	0	0	0	0	2	4	0
System Level Integration	Dual GPS Antennas	0	2	0	2	0	0	4	2	1	0	2	2	0	0
	Dual Communication	0	0	0	3	4	2	2	0	0	1	0	3	4	3
	Dual INS	0	0	0	2	4	0	1	3	4	3	0	0	0	0



[10,11,12]



Notional results

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Example: Inertial Navigation Systems

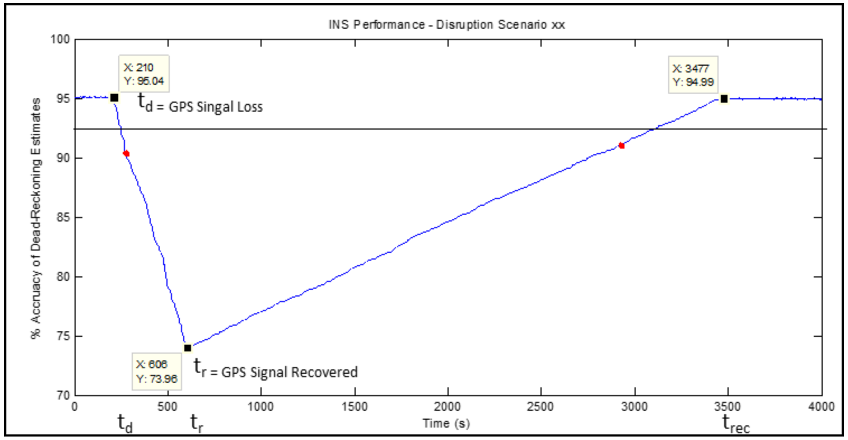
Resilience of Alternative Architectures

- Unique combinations of system elements comprise alternative architectures
- Aggregated scores for each architecture
- Resilience of each architecture based on performance variability

Architecture ID	Aggregated Heuristic Scores [h1 h2 h3 h4 h5 h6 h7 h8 h9 h10 h11 h12 h13 h14]	Avoidance	Robustness	Recovery	Resilience
001	[2 2 1 1 4 2 2 1 2 4 2 1 4 3]	0.100	0.250	0.900	0.9325
002	[1 4 0 4 1 2 2 3 3 1 0 4 1 4]	0.500	0.800	0.750	0.9825
….					
720	[4 0 4 3 4 1 3 1 3 0 0 4 2 3]	0.00	0.160	0.333	0.440

INS Capability

Maintain dead-reckoning accuracy in the face of GPS-denied environments, GPS loss, malicious jamming, and component failures.



Example: Inertial Navigation Systems

Characteristics of an Inertial Navigation System

- Air, land, and sea vehicles, including manned and unmanned systems
- Resilience needs: Avoidance and robustness key to safety critical systems

Design Principles for Engineered Resilient Inertial Navigation Systems	
Avoidance	Robustness
Reorganization Human-in-the-Loop Complexity Avoidance	Absorption Loose Coupling Physical Redundancy Functional Redundancy

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Summary of Methodology

Which design principles have been the most effective, and for which aspects of resilience?

System of Interest Research
- Components & Architectures
- Performance Variability
- Disruption Scenarios

15 comp.
720 arch.

720 arch.

Heuristics Analysis

Component Heuristics Weighted heuristic scores based on a Likert scoring system applied to patent requirements.

Aggregated Heuristic Scores
for each architecture

Resilience Analysis

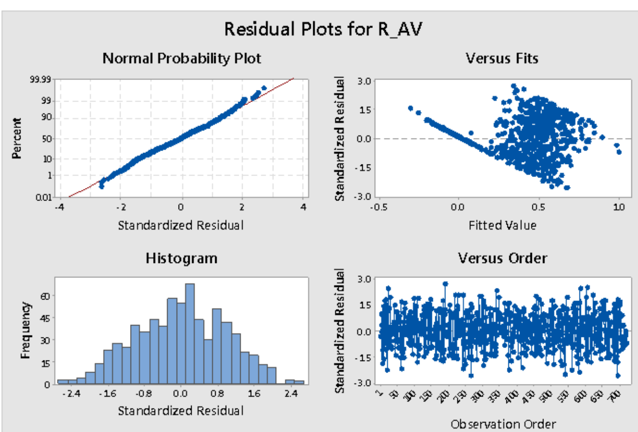
Probabilistic simulation for each architecture in the face of each disruption scenario

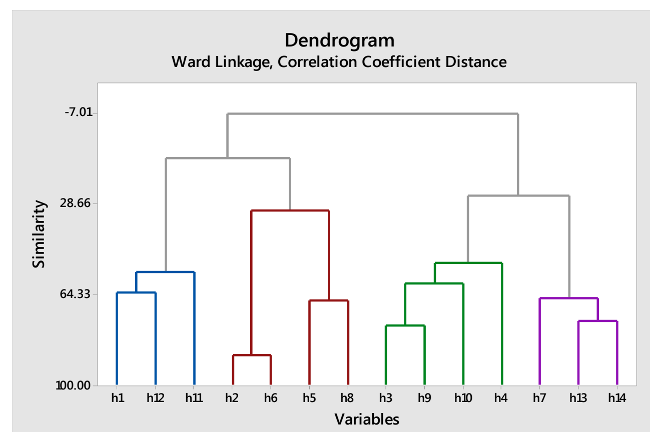
Resilience Metrics
Avoidance, Robustness, Recovery, and System Resilience

14 ordinal variables (X's) per architecture

4 continuous variables per architecture (Y's)

Relationship Models





Conclusions

- With probabilistic techniques, we can assess the capacity of a system to avoid, survive, and recover from threats
- Design principles provide systems engineering best practices for developing Engineered Resilient Systems
- Particular design approaches are identified given system characteristics and stakeholder needs.
- Safety critical systems are obvious candidates for sophisticated resilience engineering techniques.

Questions and Comments

Kenneth Stavish
kstavish@gwu.edu

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

References

1. Resilience Engineering. (2016, March 25)., *Guide to the Systems Engineering Body of Knowledge (SEBoK), version 1.6*, R.D. Adcock (EIC), Hoboken, NJ:
2. Jackson, S. & Ferris, T., (2013), *Resilience principles for engineered systems*, Systems Engineering, 2012, 15, 3, 333-346, Wiley Subscription Services, Inc., A Wiley Company.
3. International Council on Systems Engineering (INCOSE). A World in Motion - Systems Engineering Vision 2025, June 2014
4. Francis, Royce. (2012) *A metric and frameworks for resilience analysis of engineered and infrastructure systems*. Reliability Engineering & System Safety. Vol 121 90-103
5. Vugrin, E., Warren, D., Ehlen, M., and Camphouse, R. (2010) *A framework for assessing the resilience of infrastructure and economic systems*. Sustainable and Resilient Critical Infrastructure Systems: Simulation, Modeling, and Intelligent Engineering, p. 77, 2010.
6. Burch, R. (2013) *A method for calculation of the resilience of space systems.* 2013 IEEE Military Communications Conference.
7. Madni, A. & Jackson, S. (2009). *Towards a Conceptual Framework for Resilience Engineering*, IEEE Systems Journal, Vol. 3, No. 2, June 2009
8. Jackson, S. (2010) Architecting resilient systems: Accident avoidance and survival and recovery from disruptions. Edited by P. Sage, Wiley Series in Systems Engineering and Management.
9. European Organization for the Safety of Air Navigation (2009). *A white paper on resilience engineering for ATM*. September 2009
10. NASA (2016) http://mars.nasa.gov/msl; Retrieved 10 October 2016
11. How stuff works (2016) http://science.howstuffworks.com/gimbal.htm; Retrieved 10 October 2016
12. Honeywell (2016) https://aerospace.honeywell.com/en/products/navigation-and-sensors/embedded-gps-or-ins; Retrieved 10 October 2016