UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

28th Annual INCOSE international symposium
Washington, DC, USA
July 7 - 12, 2018

Fundamental Nature of Resilience of Engineered Systems

Timothy Ferris, Cranfield University
Scott Jackson, Burnham Systems Consulting
Eric Specking, University of Arkansas
Gregory Parnell, University of Arkansas
Edward Pohl, University of Arkansas

CELDi Center for Excellence in Logistics and Distribution

www.incose.org/symp2018

ERDC Engineer Research and Development Center

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

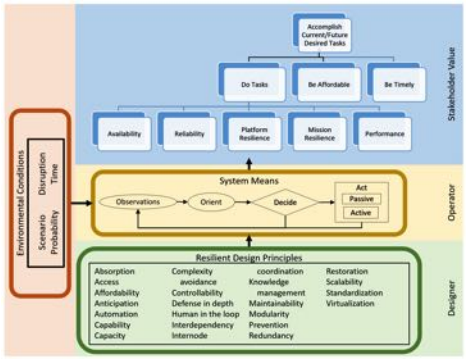
BLUF

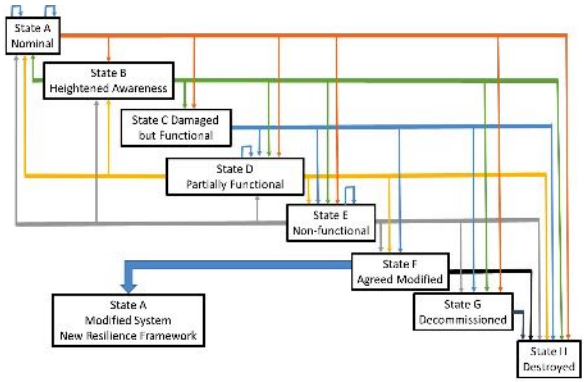
Defining Resilience

- Capability required for one system to be resilient could be significantly different than for another.
- Resilience has been defined in several ways
  - RSWG: "the ability to maintain required capability in the face of an adversity"[1]
- Resilient Engineered System
  - "a system that is able to successfully complete its planned mission(s) in the face of a disruption (environmental or adversarial), and has capabilities allowing it to successfully complete future missions with evolving threats."[2]

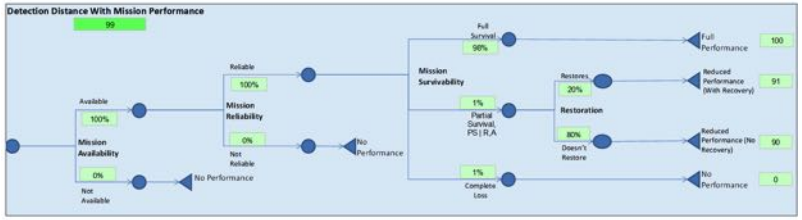
We care about what is a resilient engineered system and how to develop one.

Engineering Resilience Frameworks

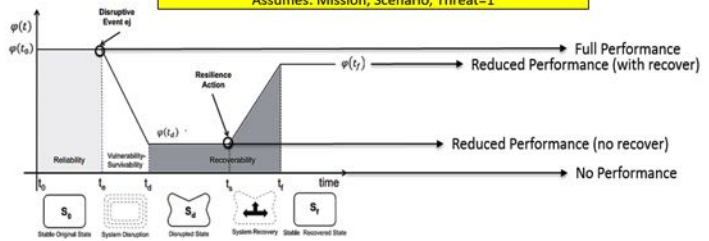




Measuring Resilience Approaches



Expected *Performance with Mission Resilience* = 98
Assumes: Mission, Scenario, Threat=1



Proposed Approach

Average across life cycle of system the expected value of the MCDA trade-off analysis of the instantaneously deliverable MOE set

1. The MCDA valuation of the MOE set achieved in each of the possible resilience conditions of the system.
2. The predicted proportion of the system life cycle duration for each of the resilience conditions in 1 above.
3. The Resilience Inclusive MCDA analysis is the sum of the products of the corresponding values for 1 and 2 above.

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

What do we need to know?

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Understanding Nature of Resilience

- Why is resilience needed/important?
- What is engineering resilience?
- Where is resilience seen?
- Who engineers resilience?
- How can a system be made resilient?
- How can resilience be measured?

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Understanding Nature of Resilience

- **Why** is resilience needed/important?
- **What** is engineering resilience?
- **Where** is resilience seen?
- **Who** engineers resilience?
- **How** can a system be made resilient?
- **How** can resilience be measured?

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Why – Accidents (environment)

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

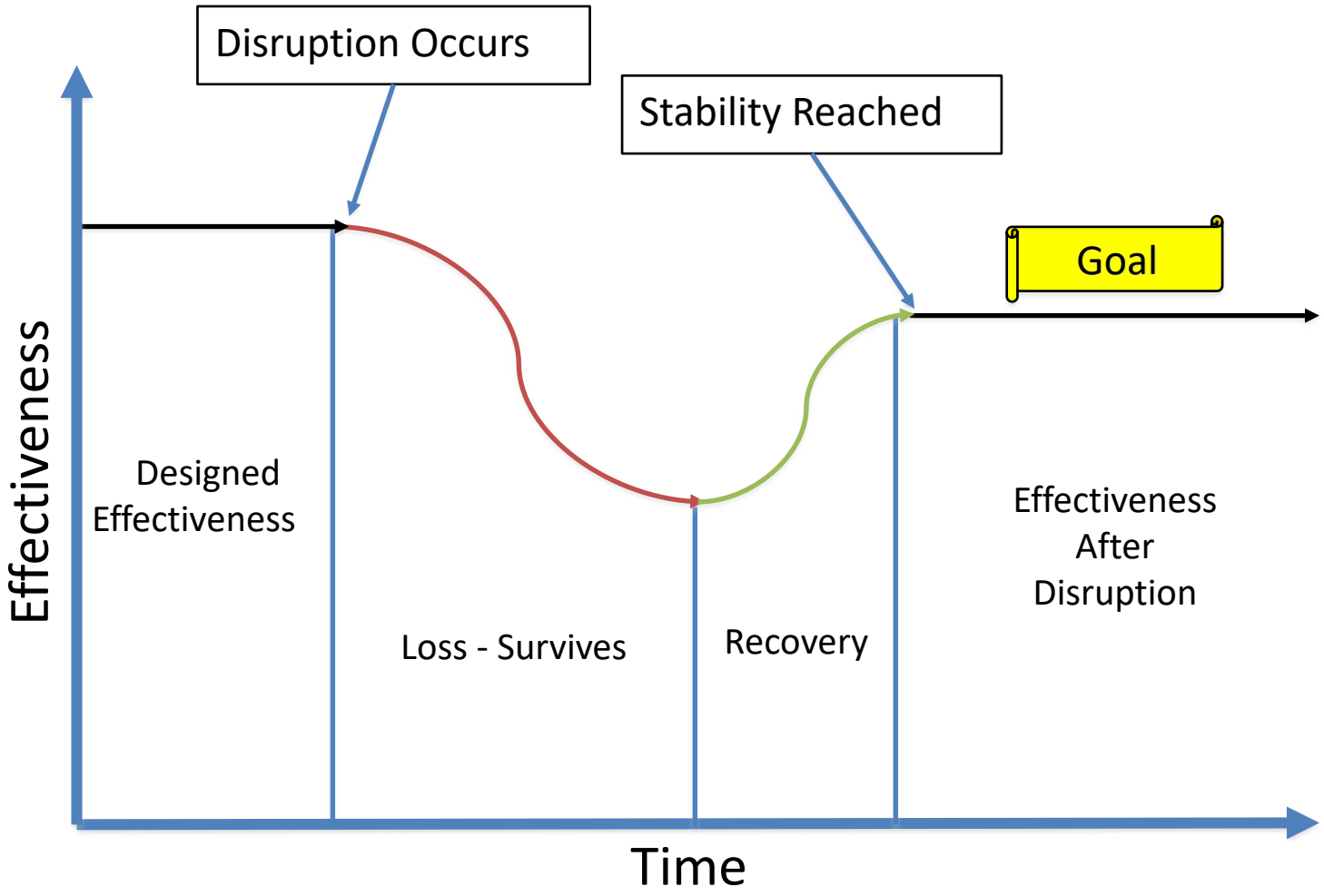
Why – Attacks (external)

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Why – Failures (internal)

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Why: System Goal

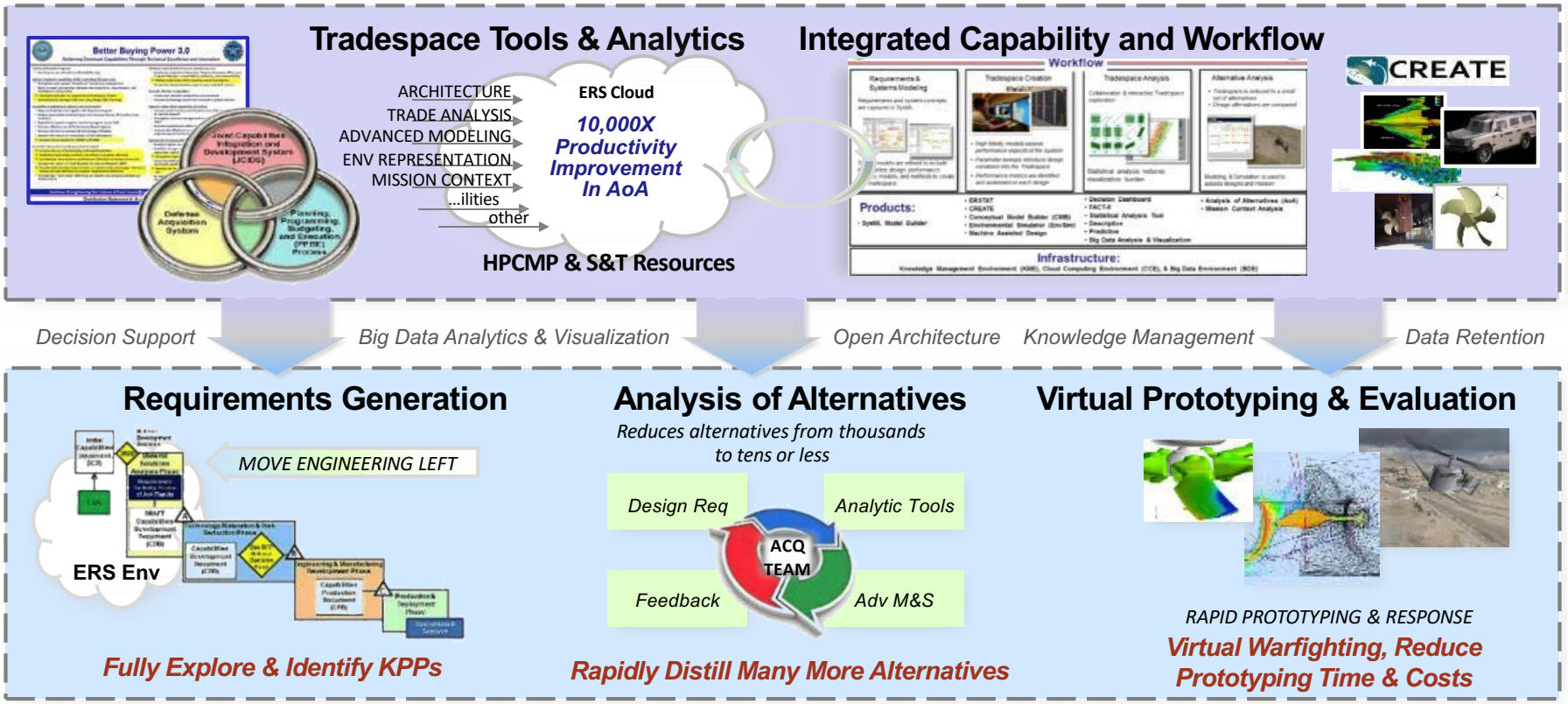


Need systems that are engineered to maintain some level of effectiveness when disruption(s) occur

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Engineered Resilient Systems

ERS is a Department of Defense (DoD) program focusing on the effective and efficient design and development of resilient complex engineered systems.



Holland, J. P. (2015). Engineered Resilient Systems: Power of Advanced Modeling and Analytics in Support of Acquisition. NDIA 16th Science and Engineering Technology Conference. Springfield, VA.

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Engineered System

- Engineered System - *"An open, concrete system of technical or socio-technical elements which is the focus of a SE life cycle . Its characteristics include being created by and for people, having a purpose and satisfying key stakeholders' value propositions when considered as part of a broader system context."* [1]

Means to enable user **capability** that provides **value** to stakeholder

[1] B. E. Board, *Guide to the Systems Engineering Body of Knowledge (SEBok)*. INCOSE, 2016.

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Capability & Value

- Capability
  - What actions and/or combinations of actions system needs to perform
  - Driven by requirements that must be verifiable
- Measure of effectiveness (MOE)
  - How well system performs its role
  - Enables capability which system is intended to provide
- Measure of performance (MOP)
  - Materiality of things that comprises the system
  - Quantities achieved in different dimensions

Proposed system design **needs** to be capable of providing the measures of performance which have been determined as necessary to enable the desired system effect assessed by a measure of effectiveness.

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Understanding Nature of Resilience

- Why is resilience needed/important?
- What is engineering resilience?
- Where is resilience seen?
- Who engineers resilience?
- How can a system be made resilient?
- How can resilience be measured?

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Defining Resilience

- Capability required for one system to be resilient could be significantly different than for another.

- Resilience has been defined in several ways
  - RSWG: "the ability to maintain required capability in the face of adversity"[1]

- Resilient Engineered System
  - "a system that is able to successfully complete its planned mission(s) in the face of a disruption (environmental or adversarial), and has capabilities allowing it to successfully complete future missions with evolving threats."[2]

We care about what is a resilient engineered system and how to develop one.

[1] B. E. Board, *Guide to the Systems Engineering Body of Knowledge (SEBok)*. INCOSE, 2016.
[2] E. Specking, M. Cilli, G. Parnell, Z. Wade, C. Cottam, C. Small, and P. E., "Tech Report: Graphical Representation of Resilient Engineered Systems," 2017.

Resilience and Ilities

- "ilities"
  - *The developmental, operational, and support requirements a program must address (named because they typically end in "ility"—availability, maintainability, vulnerability, reliability, supportability, etc.)*[1]
  - fields that contribute to the improvement of systems through the specialized analysis and design knowledge related to their particular area of concern
  - Differ from resilience in that they may utilize the same principles but have different goals
  - Provide knowledge that informs knowledge of specific aspects which contribute to resilience

Survivability

Resilience is concerned with use of all available knowledge to achieve desired system response under challenge

Resilience is focused on capability

AVAILABILITY

Maintainability

[1] INCOSE, *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. INCOSE, 2015.

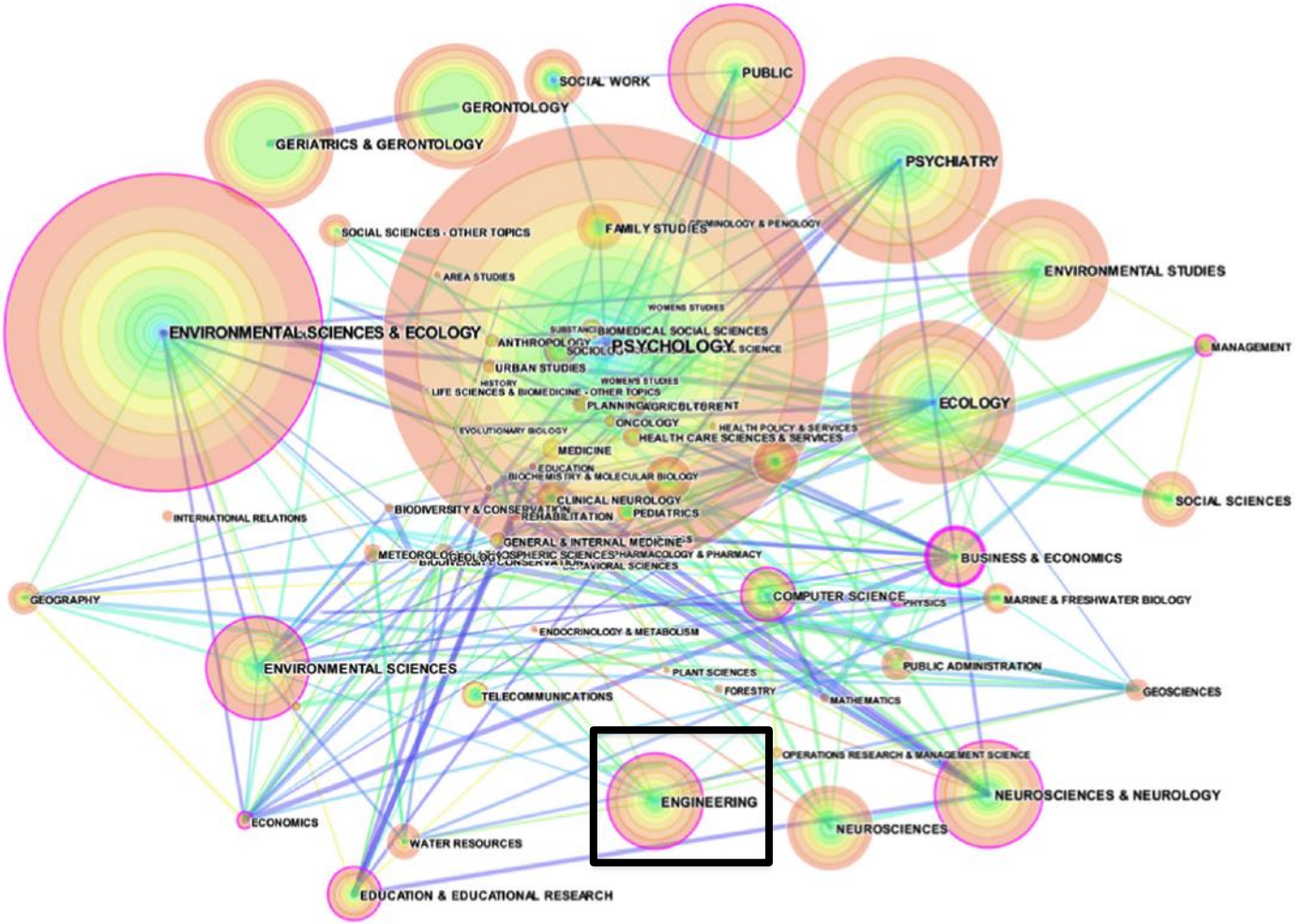
UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Understanding Nature of Resilience

- Why is resilience needed/important?
- What is engineering resilience?
- Where is resilience seen?
- Who engineers resilience?
- How can a system be made resilient?
- How can resilience be measured?

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Resilience Research

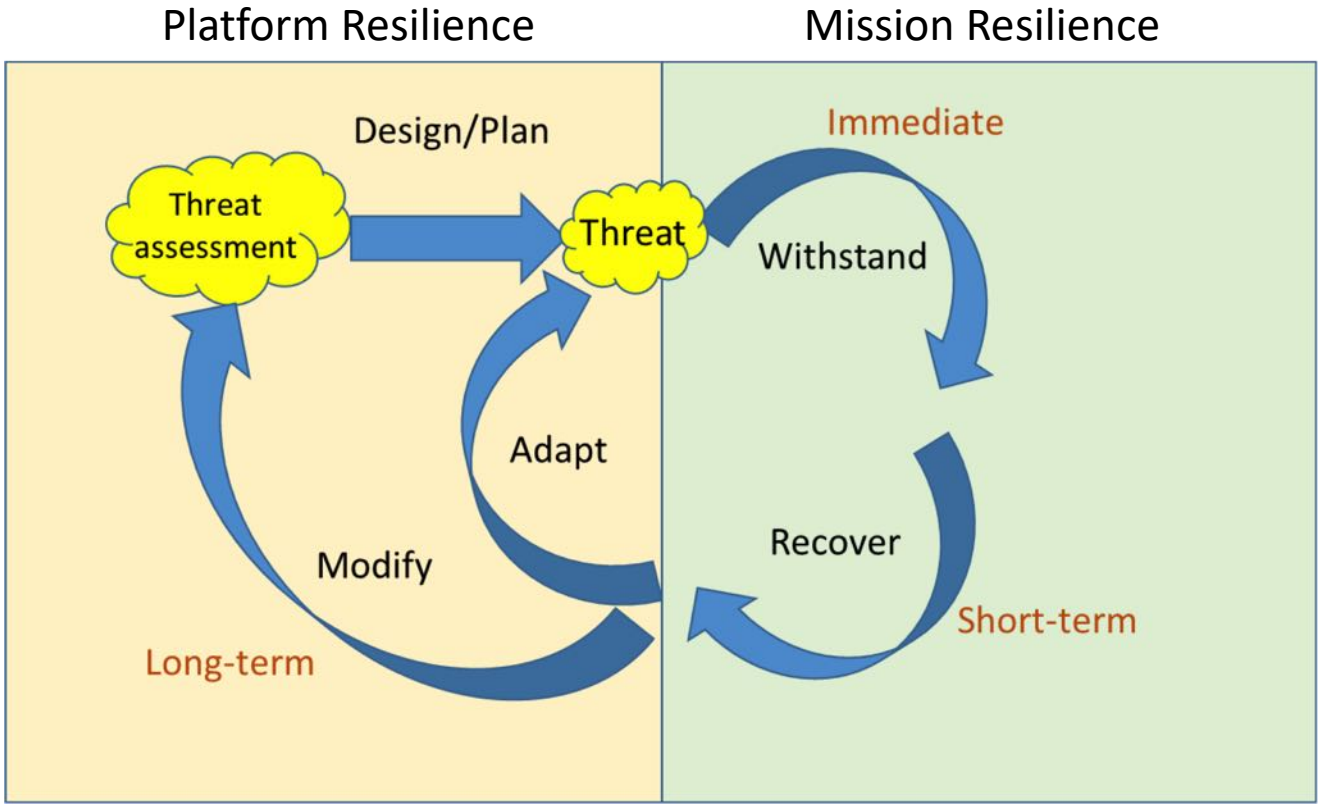


Engineering resilience is not new, but hasn't been researched as much as other fields.

S. Hosseini, K. Barker, and J. E. Ramirez-Marquez, "A Review of definitions and measures of system resilience," *Reliability Engineering \& System Safety*, vol. 145, pp. 47–61, 2016.

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Time Dimension of Resilience



After each mission the system has the potential to adapt to new threats or be modified to accommodate new functions and/or new missions.

Wade, Z., Cottam, C., Specking, E., Small, C., Parnell, G., Pohl, E., "Quantifying Resilience to Enable Resilient Systems Task 2 Technical Report" for Engineer Research and Development Center (ERDC), Center for Engineering Logistics & Distribution (CELDi), Department of Industrial Engineering, College of Engineering, University of Arkansas, January 2016

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Understanding Nature of Resilience

- Why is resilience needed/important?
- What is engineering resilience?
- Where is resilience seen?
- Who engineers resilience?
- How can a system be made resilient?
- How can resilience be measured?

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Who

Decision Makers

System Engineers

Project Managers

Designers

System Operators

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Understanding Nature of Resilience

- Why is resilience needed/important?
- What is engineering resilience?
- Where is resilience seen?
- Who engineers resilience?
- How can a system be made resilient?
- How can resilience be measured?

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Resilience: Design Concepts

Absorption
Absorption
Active damage suppression
Containment
Context spanning
Damage resistant design
Damage tolerant design
Degrade gracefully
Elasticity
Fault tolerance
Hardening
Limit Degradation
Localized capacity
Margin
Resistance
Security
Strength
Tolerance

Access
Component location
Physical accessibility

Affordability
Lifecycle Cost commensurate with perceived value
Within available budgetary constraints

Automation
Automated function
Automated reasoning techniques for executing courses of action
Autonomous reprogramming
Autonomy
Machine Intelligence

Anticipation
Agility
Anticipation
Condition monitoring
Detection
Drift correction
Fail-safe
Feedback loops
Hidden interaction avoidance
Independent Review
Threat warning

Capability
Capability
Features

Capacity
Capacity
Expandability

Complexity Avoidance
Complexity avoidance
Reduced Complexity

Controllability
Controllability
Cyber controllable components
Maneuverability
Reduce variability

Defense in Depth
Defense in depth
Layered defense

Human in the Loop
Human in control
Human in the loop
Human monitoring
Human systems integration
Neutral state

Interdependency
Cohesion
Comprehensiveness of scope
Harmonization of purposes
Holism
Interdependency
Unification

Internode Coordination
Informed operator
Intent awareness
Internode impediment
Internode Interaction
Interoperability
Knowledge between nodes

Knowledge Management
Embedded training and testing
Intellectual ability
Knowledge management

Maintainability
Expendables
Reparability

Modularity
Loose coupling
Modification
Platform reconfigurable
Modularity

Prevention
Barriers
Component shielding
Defensive countermeasures
Designs with minimum preventative maintenance
Noise jamming/deceiving
Passive damage suppression
Reduce Susceptibility
Reduce Vulnerability

Redundancy
Component redundancy
Diversity
Functional redundancy
Heterogeneity
Physical redundancy
Redundancy
Replication

Restoration
Restoration
Restructuring

Scalability
Scalability

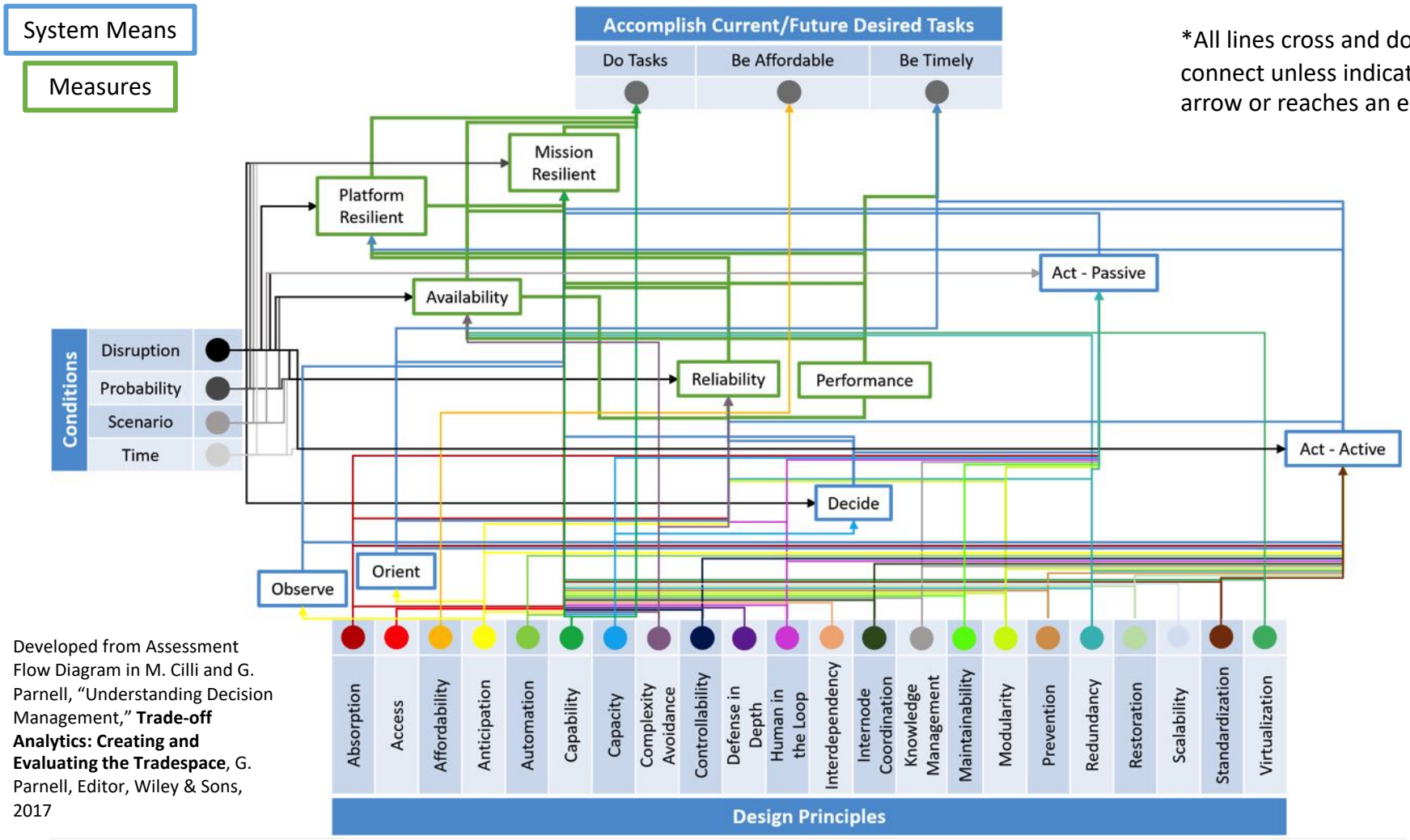
Standardization
Architectural patterns
Component elimination
Product line architectures
Standardization

Virtualization
Cloud computing
Virtualization

Specking, E., Parnell, G. S., Pohl, E., & Buchanan, R. K., "Engineering Resilient Systems: Achieving Stakeholder Value through Design Principles and System Operations," Engineering Management Journal, submitted May 18, 2018

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Resilience Principles-Means-Ends Diagram links resilience principles to performance measures



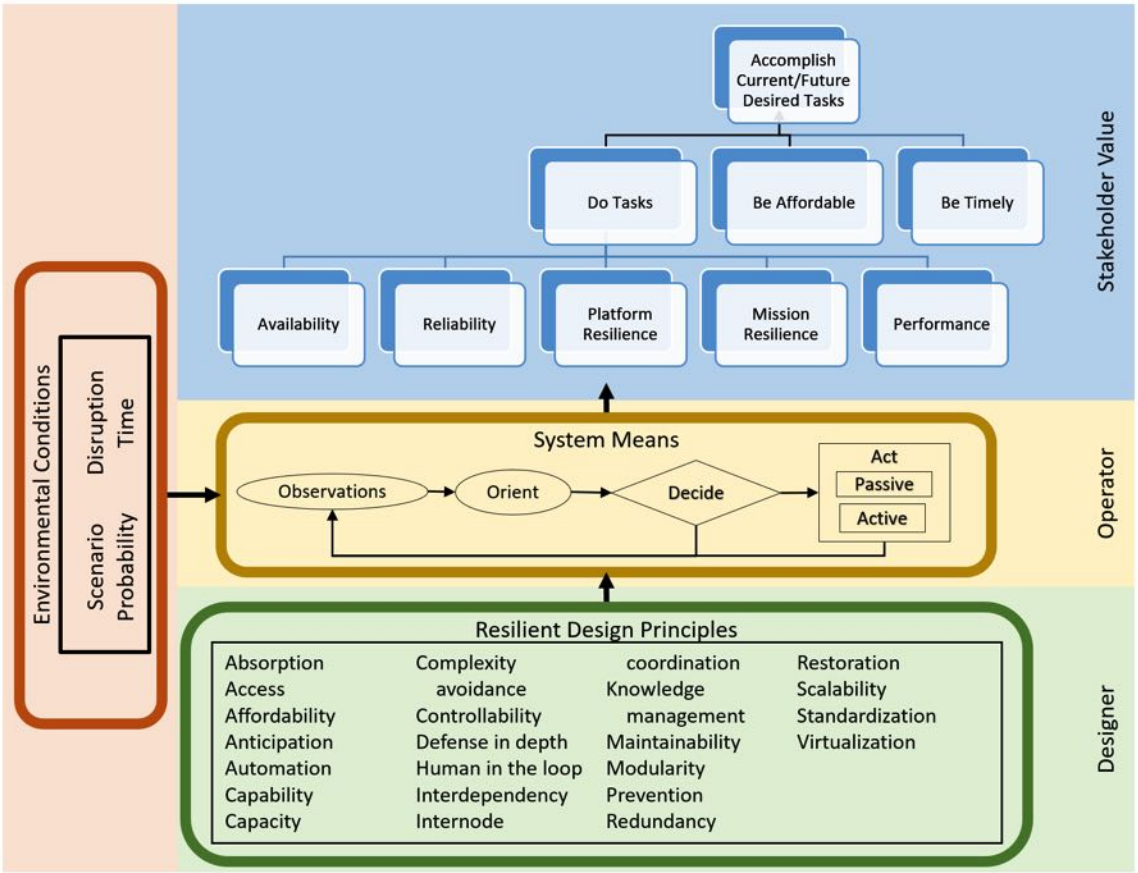
*All lines cross and do not connect unless indicated by arrow or reaches an end.

Developed from Assessment Flow Diagram in M. Cilli and G. Parnell, "Understanding Decision Management," **Trade-off Analytics: Creating and Evaluating the Tradespace**, G. Parnell, Editor, Wiley & Sons, 2017

Diagram shows how complex resilience is and the confusion in literature.

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Resilient Engineered System Principles-Means-Ends Diagram



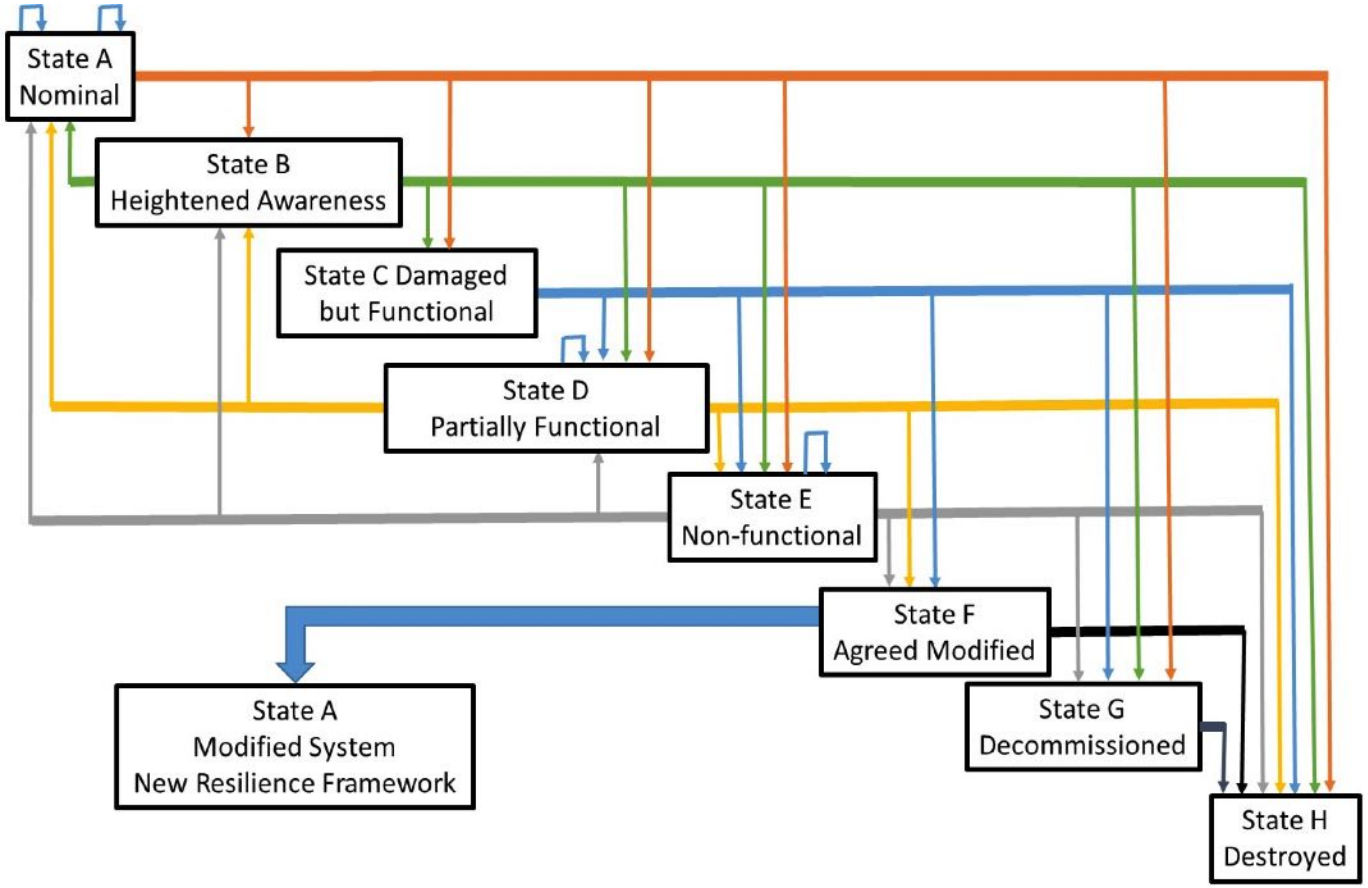
Resilience "ends" created through combination of "means" and "principles" depending upon system, mission(s), scenario(s), project time frame, and budget.

Links resilience design principles to performance measures.

Specking, E., Parnell, G. S., Pohl, E., & Buchanan, R. K., "Engineering Resilient Systems: Achieving Stakeholder Value through Design Principles and System Operations," Engineering Management Journal, submitted May 18, 2018

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

State Machine Model of Resilience



Demonstrates the variety of events and event types that could happen during a mission and the life of a system.

Highlights how to respond based upon how the disruption effects the system.

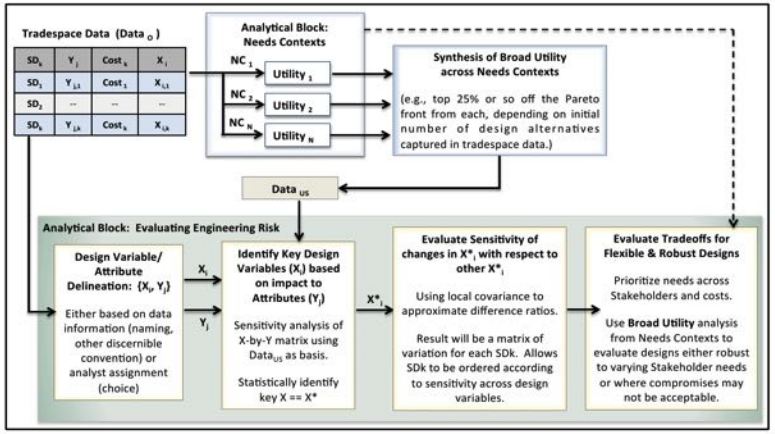
UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Understanding Nature of Resilience

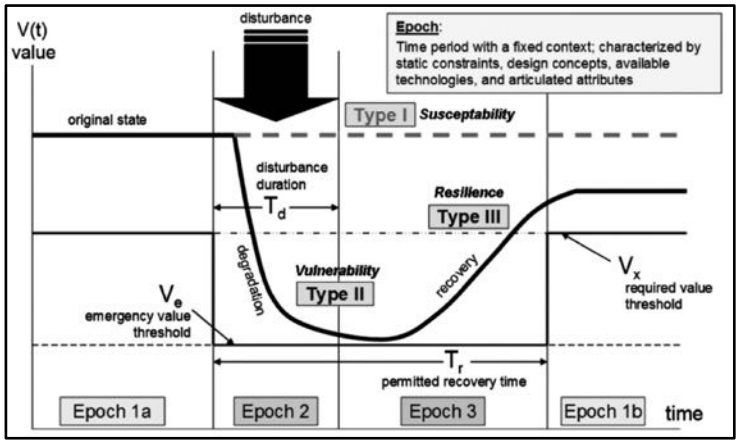
- Why is resilience needed/important?
- What is engineering resilience?
- Where is resilience seen?
- Who engineers resilience?
- How can a system be made resilient?
- How can resilience be measured?

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Measuring Resilience



Sitterle et al. Integrated Tradeoff Workflow[1]



Ross et al. Survivability Illustration[2]

$$R = \int_{t_0}^{t_1} [100 - Q(t)]\, dt$$

Equation 1 Bruneau et al. Seismic Resilience[3]

Many ways, but lack of standardized method

Examples: MCDA, fuzzy logic, stochastic modeling, modeling and simulation, and optimization techniques

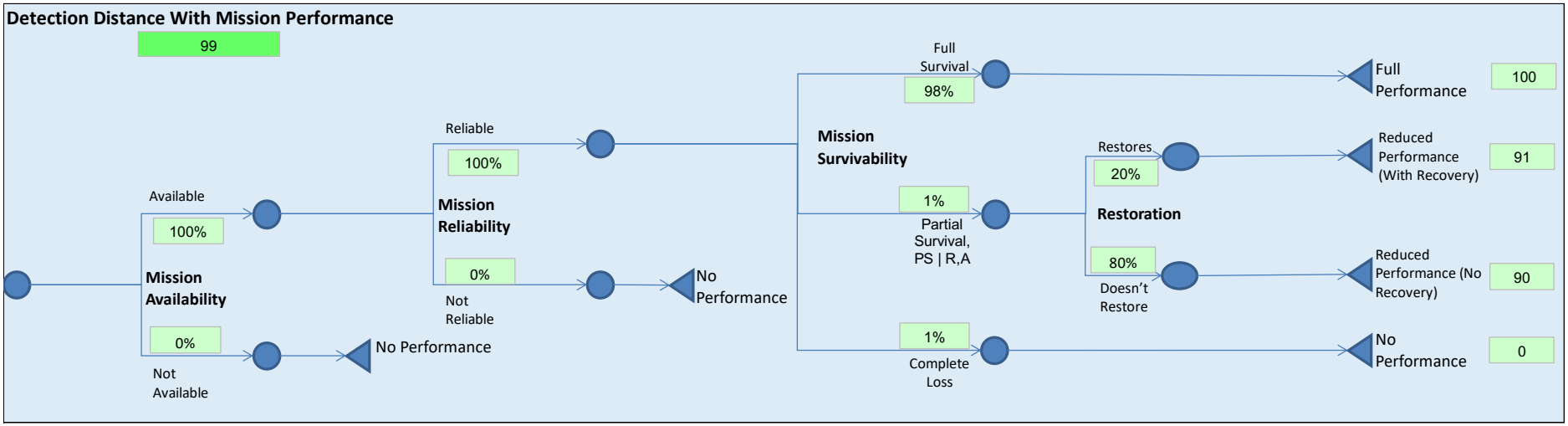
[1] V. B. Sitterle, D. F. Freeman, S. R. Goerger, and T. R. Ender, "Systems Engineering Resiliency: Guiding Tradespace Exploration within an Engineered Resilient Systems Context, " Procedia Computer Science, vol. 44, pp. 649–658, 2015.

[2] A. M. Ross, D. B. Stein, and D. E. Hastings, "Multi-Attribute Tradespace Exploration for Survivability," Journal of Spacecraft and Rockets, vol. 51, no. 5, pp. 1735–1752, 2014.

[3] M. Bruneau, S. E. Chang, R. T. Eguchi, G. C. Lee, T. D. O'Rourke, A. M. Reinhorn, M. Shinozuka, K. Tierney, W. A. Wallace, and D. von Winterfeldt, "A framework to quantitatively assess and enhance the seismic resilience of communities," Earthquake spectra, vol. 19, no. 4, pp. 733–752, 2003.

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Incorporate Resilience in all appropriate Key Performance Parameters (KPPs)



Expected *Performance with Mission Resilience* $= 98$
Assumes: Mission, Scenario, Threat=1

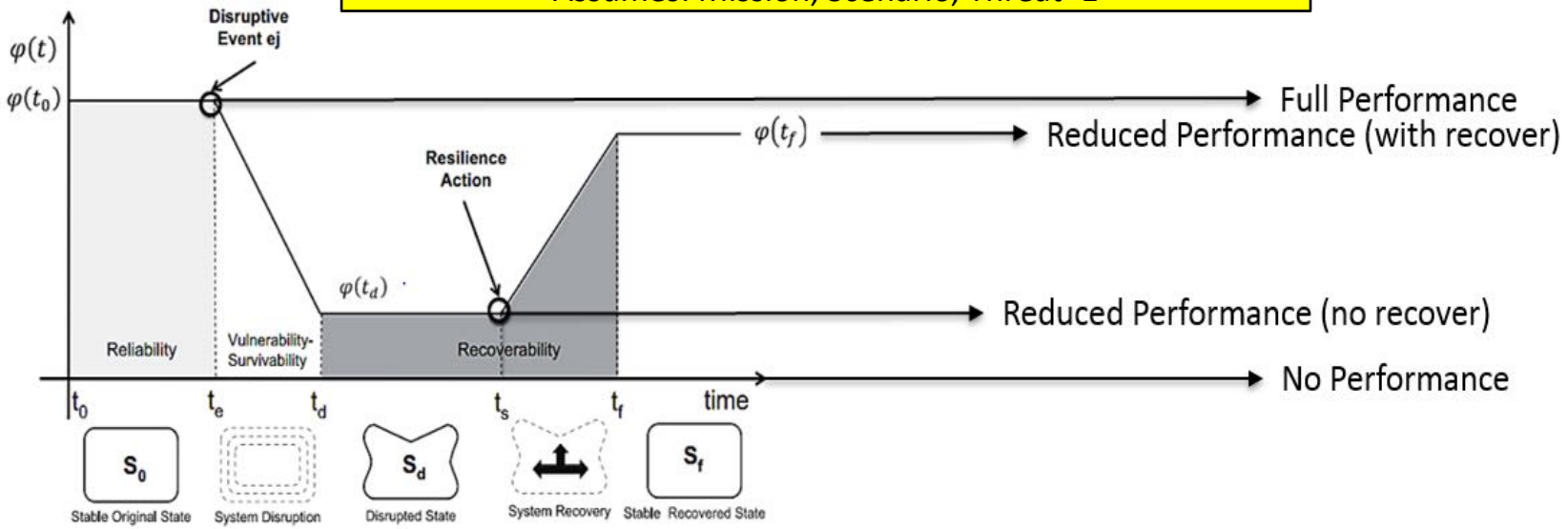


Illustration modified from Barker, K., Rocco, C. M., & Ramirez-Marquez, J. E. (2013). Resilience Based Network Component Importance Measures. Reliability Engineering & Systems Safety, 89-97.

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Proposed Approach

Average across life cycle of system the expected value of the MCDA trade-off analysis of the instantaneously deliverable MOE set

1. The MCDA valuation of the MOE set achieved in each of the possible resilience conditions of the system.
2. The predicted proportion of the system life cycle duration for each of the resilience conditions in 1 above.
3. The Resilience Inclusive MCDA analysis is the sum of the products of the corresponding values for 1 and 2 above.

UNIVERSITY OF ARKANSAS
COLLEGE OF ENGINEERING

Summary

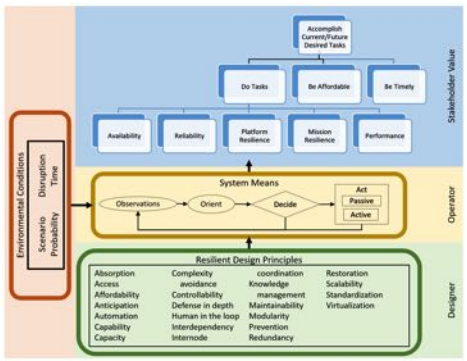
Eric Specking
especki@uark.edu
479-575-7780

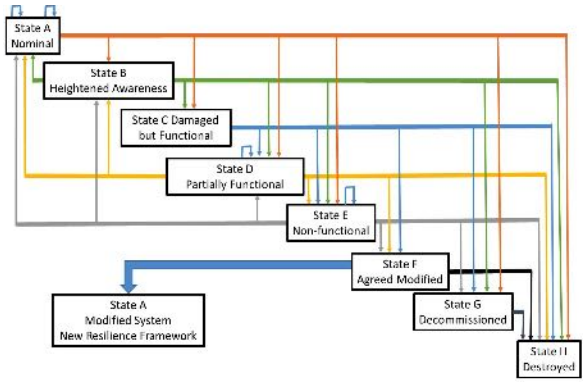
Defining Resilience

- Capability required for one system to be resilient could be significantly different than for another.
- Resilience has been defined in several ways
  - RSWG: "the ability to maintain required capability in the face of an adversity"[1]
- Resilient Engineered System
  - "a system that is able to successfully complete its planned mission(s) in the face of a disruption (environmental or adversarial), and has capabilities allowing it to successfully complete future missions with evolving threats."[2]

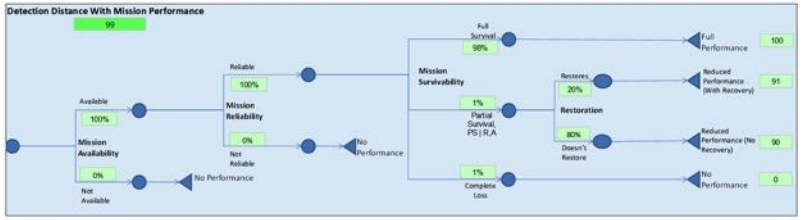
We care about what is a resilient engineered system and how to develop one.

Engineering Resilience Frameworks

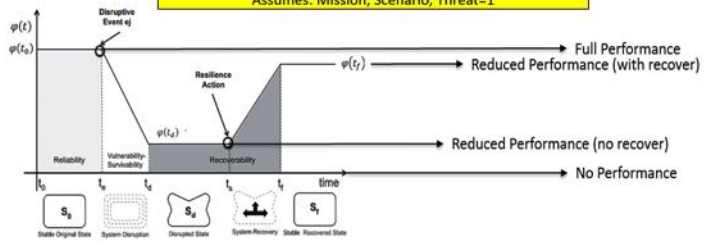




Measuring Resilience Approaches



Expected *Performance with Mission Resilience* = 98
Assumes: Mission, Scenario, Threat=1



Proposed Approach

Average across life cycle of system the expected value of the MCDA trade-off analysis of the instantaneously deliverable MOE set

1. The MCDA valuation of the MOE set achieved in each of the possible resilience conditions of the system.
2. The predicted proportion of the system life cycle duration for each of the resilience conditions in 1 above.
3. The Resilience Inclusive MCDA analysis is the sum of the products of the corresponding values for 1 and 2 above.